"strongly encourages States to submit certification packages by October 1, 2007," and sets a drop-dead date of February 10, 2008, for states to file these certification packages, which detail States' plans to fulfill the obligations detailed in the final regulations.[201] These certification packages include a "comprehensive security plan for [each State's] DMV offices and driver's license storage and production facilities, databases, and systems utilized for collecting, disseminating or storing information used in the issuance of REAL ID licenses."[202] This comprehensive security plan must also include "how the State will protect the privacy of the data collected, used, and maintained in connection with REAL ID, including all the source documents."[203] The certification packages must also include an exceptions process for people who cannot fulfill the requirements necessary to receive a REAL ID card.[204]

The two-year delay in releasing draft regulations and the short timeline for the States to create "certification packages" detailing how they will comply with the final regulations makes it virtually impossible for the States to create useful implementation plans that take privacy and security questions into consideration. This fast-track scheduling makes it appear dubious that DHS will take comments submitted by the public into account when creating the final regulations for REAL ID implementation, though the agency is required to under law.

XIV. REAL ID MUST BE REPEALED

REAL ID is fundamentally flawed because it creates a national identification system. It cannot be fixed no matter what the implementation regulations say. Therefore,

---

[201] REAL ID Draft Regulations at 10,824, *supra* note 1.
[202] *Id*. at 10,825.
[203] *Id*. at 10,825.
[204] *Id*. at 10,822.

the REAL ID Act must be repealed. Federal legislation has been introduced to repeal the REAL ID Act.[205] Arkansas, Maine, Idaho, Montana, and Washington State all have passed legislation rejecting the REAL ID Act, and more than 20 other states are debating similar legislation.[206]

The Department of Homeland Security protests that it must implement the REAL ID Act, but Homeland Security Secretary Michael Chertoff has worked with members of Congress in the past on problems with implementing the REAL ID Act.[207] He can continue to work with members of Congress to reject this national identification scheme.

XV. CONCLUSION

For the foregoing reasons, the Coalition urges the Department of Homeland Security to recommend to Congress that REAL ID is unworkable and must be repealed. The REAL ID Act creates an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties and undermines well-established principles of law found in the Privacy Act. Assuming that REAL ID is repealed, any subsequent legislation should be subjected to extensive review that explicitly addresses all of the issues raised in this document.

Respectfully submitted,

ELECTRONIC PRIVACY INFORMATION CENTER

---

[205] *See* EPIC's page on National ID Cards and the REAL ID Act page, http://www.epic.org/privacy/id_cards/ (information about federal and state legislation concerning REAL ID).

[206] *Id.*

[207] At the press conference announcing the release of the draft regulations for REAL ID implementation, Secretary Chertoff said, "And, I want to say in particular that in formulating the proposal that we're announcing today we were delighted to work closely with governors and members of Congress." Michael Chertoff, Sec'y, Dep't of Homeland Sec., Remarks at a Press Conference on REAL ID (Mar. 1, 2007), transcript *available at* http://www.dhs.gov/xnews/releases/pr_1172834392961.shtm.

AND

[EXPERTS IN PRIVACY AND TECHNOLOGY]

STEVEN AFTERGOOD
PROF. ANITA ALLEN
PROF. ANN BARTOW
PROF. JAMES BOYLE
DAVID CHAUM
SIMON DAVIES
WHITFIELD DIFFIE
PROF. DAVID FARBER
PHILIP FRIEDMAN
DEBORAH HURLEY
PROF. JERRY KANG
CHRIS LARSEN
MARY MINOW
DR. PETER G. NEUMANN
DR. DEBORAH PEEL
STEPHANIE PERRIN
PROF. ANITA RAMASASTRY
BRUCE SCHNEIER
ROBERT ELLIS SMITH
PROF. DANIEL J. SOLOVE
PROF. FRANK M. TUERKHEIMER

APPENDIX II

REAL ID Implementation Review: Few Benefits, Staggering Costs

May 2008

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

REAL ID IMPLEMENTATION REVIEW: FEW BENEFITS, STAGGERING COSTS

ANALYSIS OF THE DEPARTMENT OF HOMELAND SECURITY'S NATIONAL ID PROGRAM

ELECTRONIC PRIVACY INFORMATION CENTER

MAY 2008

REAL ID IMPLEMENTATION REVIEW: FEW BENEFITS, STAGGERING COSTS

ANALYSIS OF THE DEPARTMENT OF HOMELAND SECURITY'S NATIONAL ID PROGRAM

ELECTRONIC PRIVACY INFORMATION CENTER

MAY 2008

About EPIC

The Electronic Privacy Information Center is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.

EPIC staff

Marc Rotenberg
President & Executive Director

Lillie Coney
Associate Director & Coordinator, The Privacy Coalition

Melissa Ngo
Senior Counsel & Director, EPIC Identification & Surveillance Project

John Verdi
Staff Counsel & Director, EPIC Open Government Project

Katitza Rodríguez Pereda
Director, EPIC International Privacy Project & Coordinator, The Public Voice

Simon Davies
Senior Fellow

Harry Hammitt
Senior Fellow

Guilherme Roschke
Skadden Fellow

Daniel Burger
Administrative Director

Acknowledgements

For support of our efforts to safeguard privacy and civil liberties in the post-9/11 era, EPIC gratefully acknowledges the contributions of individual donors and the following foundations: the Ford Foundation, the Fund for Constitutional Government, the HKH Foundation, the Irving Kohn Foundation, the Albert List Foundation, the OSI, the Rockefeller Family Fund, the Scherman Foundation, the Sun Hill Foundation, and the Trio Foundation of St. Louis.

EXECUTIVE SUMMARY

Throughout its history, the United States has rejected the idea of a national identification system. Yet, the Department of Homeland Security continues to push forward a system of identification that has been widely opposed. The REAL ID Act mandates that State driver's licenses and ID cards follow federal technical standards and verification procedures issued by Homeland Security. REAL ID also enables tracking, surveillance, and profiling of the American public.

May 11, 2008 was the statutory deadline for implementation of the REAL ID system, but not one State is in compliance with the federal law creating a national identification system. In fact, 19 States have passed resolutions or laws rejecting the national ID program. The Department of Homeland Security has faced so many obstacles that the agency now plans an implementation deadline of 2017 -- nine years later than the 2008 statutory deadline.

Homeland Security claims that it is making strides in implementing the national ID program. Homeland Security Secretary Michael Chertoff encourages the use of the REAL ID system for a wide variety of purposes unrelated to the law that authorized the system. In an opinion column written by Secretary Chertoff after the publication of the final rule in January, he said, "embracing REAL ID" would mean it would be used to "cash a check, hire a baby sitter, board a plane or engage in countless other activities." None of these uses for the REAL ID have a legal basis. Each one creates a new risk for Americans who are already confronting the staggering problem of identity theft.

Last year, EPIC submitted detailed comments to the DHS on the draft proposal for REAL ID. With the assistance of many experts, we attempted to address the enormous challenge in the project proposal. In the following report, EPIC details the many problems with the final plan to implement this vast national identification system. The REAL ID system remains filled with threats to privacy, security and civil liberties that have not been resolved.

MARC ROTENBERG
EPIC EXECUTIVE DIRECTOR

MELISSA NGO
DIRECTOR, EPIC IDENTIFICATION & SURVEILLANCE PROJECT*

* *EPIC Skadden Fellow Guilherme Roschke contributed to this report.*

TABLE OF CONTENTS

I. INTRODUCTION: HISTORY OF NATIONAL IDENTIFICATION

National identification cards have long been advocated as a means to enhance national security; unmask potential criminals, chiefly terrorists; and guard against illegal immigration.[1] The cards are used in many countries including Belgium, Egypt, France, Germany, Greece, Hong Kong, Malaysia, and South Africa.[2] Currently, the United States and the United Kingdom continue to debate the merits of adopting national ID cards. The types of card, their functions, and privacy safeguards vary widely.

EPIC and Privacy International's *Privacy and Human Rights: An International Survey of Privacy Laws and Developments,* explains the basics of the technology used in national ID cards:

> In recent years technology has rapidly evolved to enable electronic record creation and the construction of large commercial and State databases. A national identifier contained in an ID card enables disparate information about a person that is stored in different databases to be easily linked and analyzed through data mining techniques. ID cards are also becoming "smarter" – the technology to build microprocessors the size of postage stamps and put them on wallet-sized cards has become more affordable. This technology enables multiple applications such as a credit card, library card, health care card, driver's license and government benefit program information to be all stored on the same national ID along with a password or a biometric identifier.[3]

During the history of the national ID card debate in the United States, Americans have consistently rejected the creation of such a system. When the Social Security Number ("SSN") was created in 1936, it was meant to be used only as an account number associated with the administration of the Social Security system.[4] Though use of the SSN has expanded considerably, it is not a universal identifier and efforts to make it one have been consistently rejected. In 1971, the Social Security Administration task force on the Social Security Number[5] declined to transform the number into an ID card.[6] The Health, Education and Welfare Secretary's Advisory Committee on Automated Personal Data Systems in 1973 again rejected the creation of a national identifier and advocated the establishment of significant safeguards to protect personal data. The committee said:

> We recommend against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems. What is needed is a halt to the drift

> toward [a standard universal identifier] and prompt action to establish safeguards providing legal sanctions against abuses of automated personal data systems.[7]

The Federal Advisory Committee on False Identification also advised against the use of a national identifier in 1976.[8] In 1977, the Privacy Protection Study Commission recommended against the adoption of a national ID system.[9] In its report, *Personal Privacy in an Information Society*, the commission said that it:

> sees a clear danger that a government record system, such as that maintained by the Social Security Administration or the Internal Revenue Service, will become a *de facto* central population register unless prevented by conscious policy decisions. Therefore […] the Federal government should act positively to halt the incremental drift toward creation of a standard universal label and central population register until laws and policies regarding the use of records about individuals are developed and shown to be effective.[10]

In Congressional testimony in 1981, Attorney General William French Smith stated that the Reagan administration was "explicitly opposed to the creation of a national identity card."[11] The Clinton administration advocated a "Health Security Card" in 1993 and assured the public that the card, issued to every American, would have "full protection for privacy and confidentiality."[12] Still, the idea was rejected and the card never was created. In 1999, Congress repealed a controversial provision in the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 that authorized the inclusion of SSNs on driver's licenses.[13]

In response to the tragic events of September 11, 2001, there has been renewed interest in the creation of national ID cards. Soon after the attacks, Larry Ellison, head of California-based software company Oracle Corporation, called for the development of a national identification system and offered to donate the technology to make this possible. He proposed ID cards with embedded digitized thumbprints and photographs of all legal residents in the U.S.[14] There was much public debate about the issue, and Congressional hearings were held. Former House Speaker Newt Gingrich testified that he "would not institute a national ID card because you do get into civil liberties issues."[15] Congress, in establishing the Department of Homeland Security, expressly prohibited the agency from developing National ID systems.[16] The Act stated simply:

> Nothing in this Act shall be construed to authorize the development of a national identification system or card.[17]

Nonetheless, the Department of Homeland Security continues to push forward with the REAL ID plan, as well as other proposals for identification and tracking.[18]

II. THE CREATION OF THE REAL ID SYSTEM

In May 2005, the REAL ID Act was appended to a bill providing tsunami relief and military appropriations and passed with little debate and no hearings.[19] It was passed in this manner even though Republican and Democratic lawmakers in the Senate urged Senate Majority Leader Bill Frist to allow hearings on the bill and to permit a separate vote on the measure.[20] The senators said they believe "Legislating in such a complex area without the benefit of hearings and expert testimony is a dubious exercise and one that subverts the Senate's deliberative process."[21] Even though Congress was unable to debate the matter, civil liberties organizations began a public dialogue shortly after passage of the REAL ID Act.[22]

When the agency released the draft regulations in March 2007, it received more than 21,000 public comments.[23] EPIC joined 24 experts in privacy and technology in submitting comments that detailed significant privacy and security problems in the draft regulations.[24] EPIC also encouraged public participation in the rulemaking process through a project organized by the Privacy Coalition, and in collaboration with over 60 organizations and more than 200 Internet bloggers.[25]

On January 11, 2008, about two and a half years after the passage of the REAL ID Act of 2005, Department of Homeland Security Secretary Michael Chertoff released the final rule to implement the national identification system created under the Act.[26] The proposal has drawn sharp criticism from State governments,[27] members of Congress,[28] civil liberties advocates,[29] and security experts.[30]

In response to the public comments to the draft regulations, the Department of Homeland Security scaled back some of the requirements, reduced the cost, and extended the deadline for State compliance in the final rule for the REAL ID system.[31] However, Secretary Chertoff continues to encourage the use of the REAL ID system for a wide variety of purposes unrelated to the law that authorized the system, including employment eligibility verification.[32] He also indicates that the agency would not prevent the use of the card by private parties for non-government purposes.[33] Also, as part of the cost-saving effort, Homeland Security decided not to encrypt the data that will be stored on the card.[34]

Though the Department of Homeland Security made some modification and attempted to solve several problems described in the public comments, the changes are not enough. REAL ID remains unworkable and should be repealed. The Department of Homeland Security is attempting to create an illegal *de facto* national identification system filled with threats to privacy, security and civil liberties that cannot be solved, no matter what the implementation plan set out by the regulations.

Even if REAL ID implementation were to go forward, the final regulations include poor privacy and security safeguards for the sensitive personal data of cardholders. The changes made in response to public comments about the proposed draft regulations are marginal, at best. For such a system to have the minimum protections necessary, the requirements of the Privacy Act of 1974 must be fully enforced for all uses of the data, current and future.[35] Agencies should not be permitted to assert any exemptions, and individuals must be granted all rights, including the judicially enforceable right to access and correct their records and to ensure compliance with all Privacy Act requirements. Moreover, technical safeguards need to be incorporated into both the identity card and the databases systems. The DHS failed to establish adequate safeguards for privacy and security.

In our May 2007 comments to Department of Homeland Security concerning the draft REAL ID regulations, EPIC listed several privacy and security problems inherent in this national identification scheme. Below, we detail how the final regulations have changed the REAL ID system and whether our criticisms were answered.

A. REAL ID Is Still Not Voluntary

The Department of Homeland Security has repeatedly stated that REAL ID is not mandatory, therefore, it is not an unfunded mandate. However, in EPIC's May 2007 comments on the draft REAL ID regulations, we explained the reasons why REAL ID is not a "voluntary" program. "States are under considerable pressure to implement REAL ID and citizens who fail to carry the new identity document will find it impossible to pursue many routine activities."[36] Also, "The administration has also pursued a heavy-handed assault on those who have raised legitimate questions about the efficacy, cost, and impact of the [REAL ID] program. [. . .] In Congressional testimony, a high-ranking DHS official said, 'Any State or territory that does not comply increases the risk for the rest of the Nation.' "[37]

In the final rule, the Department of Homeland Security does nothing to change this initial assessment. In fact, the REAL ID initiative has practically invited proposals for expanded identification requirements in the United States.[38] Though the agency limited the "official purposes" of REAL ID cards to the

statutorily mandated purposes ("boarding of Federally-regulated commercial aircrafts, entering of Federal facilities, and nuclear power plants"), the agency said it "will continue to consider additional ways in which a REAL ID license can or should be used."[39] In its discussion of the final rule, DHS also said "widespread" acceptance of the REAL ID national identification system could lead to restrictions in "access to public subsidies and benefits programs" as well as restricting access to firearms or even elections.[40] In his remarks announcing the final rule, DHS Secretary Michael Chertoff said that "it is probably reasonably predictable that as these licenses become more widely distributed," then more groups will choose to use REAL ID cards; in fact, he said they would likely "flock" to the REAL ID national identification system.[41]

The Department of Homeland Security continues its assault against States that contemplate rejection of the REAL ID national identification system. In the discussion of the final rule, the agency said it "believes that many States may find noncompliance an unattractive option" because the States would not be able to "maintain the conveniences enjoyed by their residents when using their State-issued driver's licenses and non-driver identity cards for official purposes, particularly as it pertains to domestic air travel."[42]

"That will mean real consequences for their citizens starting in May if their leadership chooses not to comply," Department of Homeland Security spokeswoman Laura Keehner said in January.[43] "That includes getting on an airplane or entering a federal building, so *they will need to get passports.*" (emphasis added).[44] This is a significant monetary penalty, as U.S. passports currently cost $85 to $100.[45] DHS itself admits that only "25% of the population already holds a valid passport."[46]

EPIC's assessment concerning the "voluntary" nature of the REAL ID national identification system remain unchanged from May. The Department of Homeland Security's declared support for and expectation of "widespread" use of the REAL ID systems, and the agency's continued pressure on the States and penalties for noncompliance prove the involuntariness of the national identification program.

B. Standards for ID Documents Remain Burdensome for Many

Under the REAL ID Act, States are required to obtain and verify documents from applicants that establish "(A) A photo identity document, except that a non-photo identity document is acceptable if it includes both the person's full legal name and date of birth. (B) Documentation showing the person's date of birth. (C) Proof of the person's social security account number or verification that the person is not eligible for a social security account number. (D) Documentation showing the person's name and address of principal residence" and "Evidence of lawful status."[47] Though DHS has made minimal

changes to the standards for identity documents that REAL ID applicants must provide, the agency has not solved the problems EPIC detailed in the May 2007 comments.

Under the final regulations, the only documents that could be accepted by the States to issue these new identity cards would be: (1) valid unexpired U.S. passport; (2) certified copy of a birth certificate; (3) consular report of birth abroad; (4) unexpired permanent resident card; (5) unexpired employment authorization document; (6) unexpired foreign passport with valid U.S. visa affixed and "the approved I-94 form documenting the applicant's most recent admittance into the United States"; (7) U.S. certificate of naturalization; (8) U.S. certificate of citizenship; or (9) REAL ID driver's license or identification card issued in compliance with the final regulations.[48] Notably, in the final regulations, the agency "has added a provision that would allow DHS to change the list of documents acceptable to establish identity following publication of a notice in the Federal Register."[49] Therefore, the Department of Homeland Security could make the identification document requirements even more burdensome at a later date.

These documents are virtually unchanged from those listed in the draft regulations, and such difficult standards for acceptable identification documents would limit the ability of some individuals to get a State driver's license. As we explained in May 2007, "There are questions as to whether some citizens could produce these documents, among them Native Americans, victims of natural disasters, domestic violence victims, the homeless, military personnel, or elderly individuals."[50] We noted that the Department of Homeland Security attempted to resolve this problem by allowing the States to voluntarily create an exceptions process for extraordinary circumstances, but "though DHS set minimum standards for data collection, retention and documentation of the transaction, the agency did not set minimum standards for eligibility, length of process, or cost of process."[51]

The document requirements create specific problems for domestic violence victims. Under the draft regulations, the demonstration of lawful status would require documents that an abuser would likely have control over.[52] Abusers of immigrants who are able to control their victims' immigration documents will be able to control the victim's ability to obtain a REAL ID card or license. EPIC urged the Department of Homeland Security to extend exceptions to those victims who must prove lawful immigration status, so that the abusers cannot use these documents to trap their victims into staying in abusive situations. We also recommended that the exception permitting those who do not have access to documents to use alternative documentation should be extended to the proof of lawful immigration status.

The REAL ID final rule is a little more sensitive to the problems of immigrant victims of domestic abuse. In the final rule, there is no requirement that records visibly indicate alternative documentation or that "full explanations" be attached when the exceptions process is invoked.[53] The Department of Homeland Security also indicates that simple explanations such as "for reasons of public safety" or other "generic expressions" may be used.[54] The exceptions process is also extended to allow determination of lawful status in the case of U.S. citizenship, but not other status.[55] However, the Department of Homeland Security leaves unaddressed the problem of immigrant women whose abusers destroy, steal or otherwise control their documents.

Also problematic is that, in the final rule, DHS explicitly removed the only substantive guidance it detailed on the exceptions process. In the draft regulations, DHS stated that persons born before 1935 might not have been issued birth certificates, so they might be eligible for the exceptions process.[56] But in the final rule, DHS removes this eligibility exemption.[57] In the final regulations, there is nothing that explains to either States or individuals how REAL ID applicants could prove eligibility (other than that the "process may not be used by non-citizens to establish lawful status in the United States"),[58] how long the process would take (days, weeks, months or even years), or if applicants could even afford the cost of the exceptions process, which would be above and beyond the already-high cost of the REAL ID card.

C. REAL ID's Data Verification Procedures Still Based on Faulty Premises

In EPIC's May 2007 comments, we detailed specific problems with the draft regulations' data verification procedures, including, 1) DHS relies on verification databases that are not available, 2) of the databases that are available, some are not widely available, 3) of the databases that are available, government and independent analyses have proven (and the Department of Homeland Security itself has admitted) that there the information in these databases are incomplete or full of errors), and 4) State DMV employees are unable and should not be forced to become federal immigration officials.[59] The final regulations promulgated by the Department of Homeland Security do not adequately address these problems.

Beyond the national identification system created by the State-to-State data exchange, two of four verification systems required are not fully deployed nationwide and third does not even exist. The database systems the States are required to verify applicant information against are: (1) Electronic Verification of Vital Events ("EVVE"), for birth certificate verification; (2) Social Security On-Line Verification ("SSOLV"), for Social Security Number verification; (3) Systematic Alien Verification for Entitlements ("SAVE"), for immigrant status verification; and (4) an as-yet uncreated Department of State system "to verify

passports, U.S. visas, and other information held by the Department of State," such as Consular Reports of Birth, and Certifications of Report of Birth.[60]

When the draft regulations were released, the only system that was available for nationwide deployment is SSOLV, and a survey of States by the National Governors Association found that even this database would need substantial improvements to be able to handle the workload that would be needed under REAL ID.[61] SSOLV depends on data gathered in a system whose mistakes are well-known, the Numerical Identification File ("NUMIDENT").[62] The Social Security Administration's Inspector General estimated that about 17.8 million records in the NUMIDENT have discrepancies with name, date of birth or death, or citizenship status.[63] About 13 million of these incorrect records belong to U.S. citizens.[64]

Federal reviews have found such data "seriously flawed in content and accuracy."[65] In an October opinion granting a temporary restraining order enjoining the Department of Homeland Security from implementing a new "no-match" employment eligibility verification proposal, the federal judge noted "the government recognizes, the no-match letters are based on SSA records that include numerous errors."[66] In the final rule, Department of Homeland Security admits there are accuracy and reliability problems in SSOLV said that it, AAMVA, and the States are working with SSA to attempt to solve these problems.[67]

In the draft regulations, DHS revealed "that only 20 States are using SAVE, and that the planned connection between SAVE and another database for foreign student status verification (Student and Exchange Visitor Information System, "SEVIS") may not be completed by the implementation deadline of May 2008."[68] Now, Department of Homeland Security claims "a majority" of States are enrolled in SAVE, but that it is still "working to modify the system" so that States can use it to implement the REAL ID national identification system.[69] The agency also says that the planned connection between SAVE and SEVIS has not been completed.[70]

EVVE is currently in pilot phase and only 11 States are participating, an increase of six more than the five States that were participating in May 2007.[71] In the draft regulations, the Department of Homeland Security based its requirements on the assumption that EVVE would be ready for nationwide expansion by the implementation deadline of May 11, 2008.[72] Now, DHS admits, "the EVVE system is not ready for full implementation. The final rule provides for additional time for States to implement EVVE or another system that provides for the verification of birth records."[73] DHS burdens the States by requiring that the States either use a system that the agency admits is not ready

for full deployment or the States themselves must create such a complex and costly system.

In the draft regulations, DHS required that the States use a State Department system to verify passports and some reports of births that was not yet created. The agency based this mandate on the assumption that the system "is eventually developed."[74] In the final rule, DHS admits the system still does not exist and says it is working "to provide a capability to verify passports, U.S. visas, and other information held by the Department of State."[75]

DHS states in the final rule that "States cannot and will not be required to use systems that are not fully operational and available for use," yet the agency then details mandates for the States to use systems that are not fully operational and available for use.[76] It is clear that the agency has not solved the significant problems with its verification databases and has ensured that even States that wish to implement REAL ID will confront substantial obstacles and may not be able to do so.

There is a further problem with the revised verification procedures: the Department of Homeland Security anticipates that State DMV employees will become Federal immigration officials.[77] The Department of Homeland Security has not adequately addressed these problems in its final rule for the implementation of the REAL ID national identification system.

Under the final rule, State DMV employees would still be required to verify REAL ID national identification card applicants' source documents. DHS defined "verification" as "two interrelated procedures: (1) inspection to see if the document is genuine and has not been altered, and (2) checking to see that the identity data on the document is valid."[78]

Under the final regulations, the source documents that would be accepted by the States to issue these new identity cards would be: (1) valid unexpired U.S. passport; (2) certified copy of a birth certificate; (3) consular report of birth abroad; (4) unexpired permanent resident card; (5) unexpired employment authorization document; (6) unexpired foreign passport with valid U.S. visa affixed and "the approved I-94 form documenting the applicant's most recent admittance into the United States"; (7) U.S. certificate of naturalization; (8) U.S. certificate of citizenship; or (9) REAL ID driver's license or identification card issued in compliance with the final regulations.[79] As we noted above, in the final regulations, the agency "has added a provision that would allow DHS to change the list of documents acceptable to establish identity following publication of a notice in the Federal Register."[80] Therefore, the document verification requirements could become even more burdensome for State DMV employees.

State DMV employees would be required to verify these source documents, including Federal immigration documents, though this is a complex and confusing area of law. In the draft regulations, DHS sought to solve this problem by requiring that DMV employees handling source documents undergo 12 hours of "fraudulent document recognition" training.[81] The final rule mandates "Fraudulent document recognition training for all covered employees handling source documents or engaged in the issuance of driver's licenses and identification cards."[82]

A Government Accountability Office review of the Social Security Administration found that staff had difficulty recognizing counterfeit documents, though it is their primary job to verify these documents before issuing Social Security numbers.[83] For example, the Government Accountability Office reported difficulty with detection of fraudulent birth certificates. In one case, a fake in-State birth certificate was detected, but "SSA staff acknowledged that if a counterfeit out-of-State birth certificate had been used, SSA would likely have issued the SSN because of staff unfamiliarity with the specific features of numerous State birth certificates."[84]

We reiterate what we said in our May 2007 comments, "It is questionable how well State DMV employees would be able to spot fraudulent documents, especially documents as rarely seen as consular reports of birth abroad […] when it is difficult for counterfeit documents to be spotted by federal employees whose primary job is verification of source documents."[85] It still remains unclear would happen if a State DMV employee determines that an applicant's source documents are fraudulent: What recourse would the applicant have to prove her documents are real? In the final regulations, the Department of Homeland Security again has punted its Privacy Act obligations, including appropriate redress procedures.

III. HOMELAND SECURITY HAS ABDICATED ITS RESPONSIBILITY TO PROTECT INDIVIDUAL PRIVACY

The Department of Homeland Security has stated that it is constrained in its power to protect the privacy of individuals and their data under the REAL ID Act. The agency claimed in the draft regulations that, "The Act does not include statutory language authorizing DHS to prescribe privacy requirements for the state-controlled databases or data exchange necessary to implement the Act."[86] We agree with Sen. Joseph Lieberman, who said, "The concept that federal agencies need explicit Congressional authorization to protect Americans' privacy is just plain wrong. In fact, our government is obligated to ensure that programs and regulations do not unduly jeopardize an individual's right to privacy."[87]

The final regulations create a national identification system that affects 245 million license and cardholders nationwide, yet DHS is hesitant to ensure strong privacy safeguards in the system itself. The agency has the obligation to protect the privacy of individuals affected by this system and must do more than the feeble attempts set out in the draft regulations.

The Privacy Act of 1974 applies to the entire national identification system under guidelines set out by the Office of Management and Budget ("OMB") and the Department of Homeland Security itself.[88] The OMB guidelines explain that the Privacy Act "stipulates that systems of records operated under contract or, in some instances, State or local governments operating under Federal mandate 'by or on behalf of the agency . . . to accomplish an agency function' are subject to . . . the Act."[89] The guidelines also explain that the Privacy Act "make[s] it clear that the systems 'maintained' by an agency are not limited to those operated by agency personnel on agency premises but include certain systems operated pursuant to the terms of a contract to which the agency is a party."[90] The REAL ID system is operated under a Federal mandate to accomplish several agency functions, including immigration control.

The REAL ID system is covered by the Privacy Act under the Department of Homeland Security's own policies. In a policy guidance memorandum from the agency's Privacy Office, "DHS Information Systems" is defined as "an Information System operated, controlled, or directed by the U.S. Department of Homeland Security. This definition shall include information systems that other entities, including private sector organizations, operate on behalf of or for the benefit of the Department of Homeland Security."[91] The national system of interconnected State databases is "operate[d] on behalf of or for the benefit" of DHS. The Privacy Office also states:

> As a matter of DHS policy, any personally identifiable information (PII) that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS shall be treated as a System of Records subject to the Privacy Act regardless of whether the information pertains to a U.S. citizen, Legal Permanent Resident, visitor, or alien.[92]

If the Department of Homeland Security creates this system, the agency must fully apply Privacy Act requirements of notice, access, correction, and judicially enforceable redress to the entire REAL ID national identification system. The final regulations conclude that individuals should attempt to exercise their rights to notice, access, correction and redress through State DMVs, the Social Security Administration, the Department of State, and the U.S. Citizenship and Immigration Service (a part of the Department of Homeland Security).[93]

Once again, the Department of Homeland Security has punted the issue of privacy to the States, but the agency needs to lead. Various questions remain, including important ones concerning redress. How will redress be adjudicated if one State includes erroneous information in an individual's file and passes that information on to another State? Will the individual have to petition both States separately for redress? Will neither State process the redress, because each believes it to be the responsibility of the other? The right of redress must be judicially enforceable. The Privacy Act protections must be mandated in the REAL ID implementation regulations in order for the Department of Homeland Security to fulfill its obligations.

A. Unfettered Access to 2D Barcode Data Threatens Individual Privacy

There are significant threats to individual privacy and security that would be created by unfettered access to REAL ID national identification system data.[94] Some of the problems are based on the design of the card and the safeguards for the underlying databases. Though the Department of Homeland Security has made some changes in the final rule, substantial problems remain.

Under REAL ID, the following data elements, at a minimum, must be on the REAL ID card: (1) full legal name; (2) date of birth; (3) gender; (4) driver's license or identification card number; (5) digital photograph of the person; (6) address of principal residence; (7) signature; (8) physical security features; (9) a common machine readable technology, with defined minimum data elements; and, (10) card issuance and expiration dates.[95] The REAL ID card will include a 2D barcode as its machine-readable technology, which will include elements 1 through 7 and 10, with these notations, "(b) Full legal name, unless the State permits an applicant to establish a name other than the name that appears on a source document, pursuant to Sec. 37.11(c)(2)"; "(f) Address as listed on the card pursuant to Sec. 37.17(f)"; "(h) Card design revision date, indicating the most recent change or modification to the visible format of the driver's license or identification card"; "(i) Inventory control number of the physical document"; and, "(j) State or territory of issuance."[96]

We support the Department of Homeland Security in its rejection of radio frequency identification (RFID) technology as the machine-readable technology for the REAL ID national identification card. Multiple reports, including the recommendations of the Department's own Data Privacy and Integrity Advisory Committee, made clear that RFID should not be used for human identification.[97] However, the Department's decision to leave the 2D barcode unencrypted creates unnecessary security risks.[98] In doing so, the Department of Homeland Security rejects the advice of independent privacy and security experts and the agency's own Privacy Office. The DHS Privacy Office supported encryption "because 2D bar code readers are extremely common, the data could be captured from the driver's licenses and identification cards and accessed by unauthorized

third parties by simply reading the 2D bar code on the credential" if the data is left unencrypted.[99]

There are many examples of unauthorized users being able to download data from unencrypted machine-readable technology.[100] One case involved New York prosecutors charging 13 people with harvesting data from unencrypted, machine-*readable* credit cards and clubs downloading all data contained on unencrypted State licenses.[101] To protect privacy and improve security, this machine-readable technology must either include encryption or access must be limited in some other form. As we explained earlier, "Leaving the machine readable zone open would allow unfettered third-party access to the data and leave 245 million license and cardholders nationwide at risk for individual tracking."[102]

The Department of Homeland Security rejected encryption in the final rule because of "the complexities and costs of implementing an encryption infrastructure."[103] We anticipated this and detailed a privacy-protective alternative to encryption, yet the agency did not take this path either. We said:

> We suggest that no personal data be placed on the machine readable zone. Instead, place a new identifier that is unused elsewhere (*i.e.*, not the driver's license number or Social Security Number). This unique identifier will "point" to the records in the national database. Access to the database can be controlled by password and encryption security, because it is easier to regulate public keys in this scenario. Also, the State should ensure that a new unique identifier is created each time the machine readable zone is renewed or reissued, in order to make the identifier less useful as an everyday ID number – people would not be forever linked to this identifier. This approach would improve data security and privacy.[104]

Instead of accepting this simple, privacy-protective suggestion, the Department of Homeland Security chose to require that a great deal of personal data be stored on the 2D barcode.

DHS is required to include security protections on the REAL ID card. Under the REAL ID Act, the card must include "(8) Physical security features designed to prevent tampering, counterfeiting, or duplication of the document for any fraudulent purpose."[105] The agency has this obligation and it should not abdicate this responsibility. If DHS does not seek to limit access to the data on the REAL ID card, then it is signaling that it is acceptable for third parties to download, access and store data for purposes beyond the three official purposes.

Rejecting encryption for the 2D barcode helps to push the REAL ID system into "widespread" use in everyday life, a goal that DHS Secretary

Chertoff and the DHS final rule itself expect and support. Such an expansion would harm both individual privacy and security and quickly turn the United States into a country where the REAL ID national identification card is involuntarily carried by everyone.

B. REAL ID Increases Both Insider and Outsider Threats

Under REAL ID, the government would have easy access to an incredible amount of personal data stored in one national database (or, according to the final regulation from Department of Homeland Security, 56 State and Territory databases, each of which can access all others through a "hub"-based network).[106] As it did in the draft regulations, in the final regulations DHS claims that it is not expanding data collection and retention, but it is enlarging schedules and procedures for retention and distribution of identification documents and other personal data. This broad expansion of data collection and retention in a national database creates significant threats to privacy and security.

The Department of Homeland Security justifies the expanded data collection on the misleading representations that 1) "most States" already gather, retain and distribute such extensive personal data and documents, and 2) the REAL ID national identification system does not give States or the Federal government greater access to sensitive personal data and documents than before.[107] The REAL ID national identification system mandates increased data gathering, retention and distribution, as well as massively expanding the Federal and State access to this data. The personal data of 245 million State license and ID cardholders would be accessible from a massive number of DMVs across the country.

Consolidating identity through a single document increases risks when the document is compromised. It would be as if you used one key to open your house, your car, your safe deposit box, your office, and more.[108] "Perversely – a harder-to-forge card makes subverting the system even more valuable. Good security doesn't try to divine intentionality from identification, but instead provides for broad defenses regardless of identification," such as airport screening, walls and door locks, security expert Bruce Schneier has said.[109]

There are a number of "insider" and "outsider" threats to the massive identification database connecting 56 States and territories. Creating a national identification database containing personal data of 245 million State license and ID cardholders nationwide, one that would be accessible from a massive number of DMVs across the country, is an invitation for all criminals – whether identity thieves or terrorists – to break into just one of these entrance points to gather such data for misuse.

Such a system would also be at risk of abuse from authorized users, such as DMV employees, who are bribed or threatened into changing the system data or issuing "authentic" national identification cards. It is appropriate to note here that, on the day that DHS released the final regulations for REAL ID, "A Maryland Motor Vehicle Administration employee […] and four others were indicted [ ] on charges that they made and sold fake State driver's licenses and identification cards in exchange for money."[110]

Identity theft is a large and growing problem. A Federal Trade Commission report estimated 8.3 million victims in 2005 (the last year for which numbers are available).[111] Serious cases of identity theft cost victims $1,200 - $2,500.[112] In 10 percent of new account frauds, victims incurred at least $3,000 in out-of-pocket expenses.[113] Domestic violence survivors are particularly vulnerable because their economic situation may be more precarious than average, and they may have greater need for unsullied credit as they attempt to create independent economic lives.

Large-scale data breaches have occurred in State DMVs across the country; if the databases are linked under REAL ID, these breaches will only grow in scale. The Oregon DMV lost half a million records in 2005.[114] Also that year, in Georgia, a dishonest insider exposed 465,000 records.[115] In 2006, a computer with the personal data of 16,000 individuals was stolen from a North Carolina DMV.[116] The list goes on, and the personal information of individuals will be endangered under the REAL ID national identification system.

Domestic violence survivors are particularly vulnerable. Domestic violence survivors who flee their abusers, crossing into different States, would be exposed if their abuser breaches the security of any one of these 56 interconnected databases. "An abuser with an associate inside a State DMV, law enforcement, or other agency with access to the State records would be able to track a victim as the victim moves across the country."[117]

Intentional breaches by outsiders or authorized insiders abusing their power would also have a wider scope under the Department of Homeland Security's REAL ID national identification system. Past abuses exemplify what can be expected in a nationwide scale. For example, in September, a former Department of Commerce agent was indicted and charged with using a federal database to stalk a former girlfriend and her family.[118] While employed at the Commerce Department, the agent is alleged to have accessed the system at least 163 times during a 10-month period.[119] In Arizona, a police officer admitted accessing motor vehicle records to find personal information on women he was romantically interested in, as well as co-workers.[120]

The danger of negligent and accidental disclosures is increased by REAL ID, as substantially more government employees will have access to all motor vehicle records nationwide. One example of accidental disclosure occurred in Wisconsin in 2007 – a police officer disclosed a victim's address, found in a DMV record to a stalker; the officer did not know that the victim had a restraining order against this man.[121] This sort of inadvertence will happen much more frequently in a post-REAL ID world as the access to driver's license information is spread throughout the national identification system.

C. Background Check Procedures Fail to Address Insider Threat Problems

The Department of Homeland Security requires certain government employees undergo criminal history background checks and list particular offenses that would disqualify an individual from specific jobs related to the REAL ID national identification system.[122] In the draft regulations, DHS said employees who had to undergo these checks would be limited to those who could affect the recording of information, the manufacture of REAL ID cards, or the information displayed on a card.[123] Employees who could access the record information without the ability to edit it are not subject to the background check requirement.

EPIC explained in our May 2007 comments, "This massive loophole greatly increases the security and privacy risks of domestic violence and sexual abuse victims, as significant damage can be done by unauthorized data disclosure."[124] We proposed that "the broad category of those who have access to records should be shrunk, rather than increasing the category of those who are covered by the background check requirement" in order to safeguard against these threats.[125] However, the final rule did not use this proposal.

In the draft regulations, the suitability criteria of the background check did not match the threat of stalkers and abusers. DHS proposed using the permanent and interim disqualifying criteria in the Transportation Security Administration's background checks for maritime and land transportation security at 49 C.F.R. 1572.103.[126] The offenses include espionage, sedition, treason, making bomb threats, and crimes involving transportation security incidents.[127] Some of the offenses, such as fraud and misrepresentation – including identity fraud – are relevant to the risks of improper disclosure and access to the records.[128] However, crimes such as stalking, surveillance, harassment and domestic abuse are not in this list.

Recognizing the risk of improper access to the record system, EPIC recommended that, "these crimes must be added to the list of disqualifying offenses, so that the REAL ID system does not create a loophole permitting abusers access to a national database that would allow them to track their victims no matter where the victims moved."[129] The Department of Homeland Security

did not add these offenses, allowing even convicted abusers the opportunity to access to the massive national database created under REAL ID.[130]

D. Final Rule Includes Marginal Improvements for Address Confidentiality and Name History Problems

Many States have created formal Address Confidentiality Programs and also provided general measures of residential address privacy, but these protections would be removed by the draft regulations.[131] The final rule improves on some of the address confidentiality provisions of the proposed rule, but the subject of addresses in the national ID database is treated in contradictory manners in different parts of the final rule.

The REAL ID Act requires that driver's licenses include a person's "address of principle residence."[132] This requirement effectively destroys State address confidentiality programs. The Violence Against Women and Department of Justice Reauthorization Act ("VAWA") included a requirement for DHS to "consider and address" the needs of certain groups when the agency is "developing regulations or guidance with regard to identification documents, including driver's licenses."[133] These groups include domestic violence and sexual assault victims who are entitled to be enrolled in State address confidentiality programs; whose addresses are entitled to be suppressed via court order or State or Federal law; or whose information is protected from disclosure according to Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act 1996.[134]

In the final rule, the Department of Homeland Security includes more exemptions and extends them to the unencrypted machine-readable zone. Now exempt are individuals for whom State law, regulation, or DMV procedure permits display of an alternative address.[135] This exemption includes States that generally permit a mailing address to be displayed on the card. Individuals who are enrolled in address confidentiality programs, who have their information suppressed by court orders (including administrative orders), and those who are also protected by Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 may also use an alternative address.[136] The unencrypted machine-readable zone requires the "address as listed on the card pursuant to § 37.17(f)" which includes the alternative address provisions.[137] Further, the final regulations require two documents that show "address of principle residence" but exempt street addresses pursuant to § 37.17(f), the section on that regulates address confidentiality.[138]

The agency's comments to the final rule state, "true addresses must be captured and stored in a secure manner in the DMV database even if an alternate address appears on the face and MRZ portions of the driver's license or identification card."[139] However, the actual regulation that describes the design

of the national identification database, § 37.33, does not appear to incorporate these requirements. Under § 37.33 the database must contain:

> (1) All data fields printed on driver's licenses and identification cards issued by the State, individual serial numbers of the card, and SSN;
> (2) A record of the full legal name and recorded name established under Sec. 37.11(c)(2) as applicable, without truncation;
> (3) All additional data fields included in the MRZ but not printed on the driver's license or identification card; and
> (4) Motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on driver's licenses.[140]

The gathering, retention and distribution of addresses in the databases are unclear, as the Department of Homeland Security has made contradictory statements.

Though the treatment of name history is improved in the final rule, a significant problem remains. Name histories may be kept in motor vehicle databases and thus exposed to security breaches by insiders with access or outsiders who break into any one of the many DMVs across the country with access to the national database.

The final rule allows State law or regulation to permit the use of a name other than the one on the source documents.[141] The State may itself determine what evidence is needed for it to accept the name if it differs from source documents.[142] Further, the name difference from the source document must be recorded.[143] The final regulations also permit the name on the face of the card and in the machine-readable zone to deviate from the name on source documents.[144] These are all improvements over the draft regulations.

However, the final rule for implementation of the REAL ID system still contains a problematic name history provision. The DMV database is required to have "a record of the full legal name and recorded name established under §37.11(c)(2) as applicable, without truncation."[145] This record includes copies of source documents and any evidence of a name change.[146] Such data gathering, retention and distribution would leave a trail for abusers to follow.

IV. REAL ID SYSTEM CREATES NEW NATIONAL SECURITY RISKS

The Department of Homeland Security continues to claim that the national identification system created under the REAL ID scheme will improve national security. When releasing the final rule in January, Secretary Chertoff said, "secure identification is an essential way of ensuring that people are who they say they are. And therefore this kind of identification gives us a tremendous

tool in preventing dangerous people from getting on airplanes or getting into federal buildings."[147] Yet there is a multitude of evidence that Secretary Chertoff is wrong – including evidence from the 9/11 Commission.

DHS's national security rationale has always been confusing and has not changed since the draft regulations were released in March 2007. Our May 2007 comments included a detailed debunking of the Department of Homeland Security's mystifying quantitative risk assessment.[148] The agency claimed this assessment proved the need for, cost-effectiveness of, and security advantages of the REAL ID national identification system.[149] Yet , DHS admitted at the time, "REAL ID is highly unlikely to impact the consequences of a successful attack, but it may impact, on the margin, the chance of a terrorist attack being attempted and succeeding."[150] DHS attempted to determine the *marginal* chance that REAL ID will lessen the chance of success or discourage the attempt of a terrorist attack, using a number of faulty assumptions.

In the final regulations, the Department of Homeland Security again attempts a national security rationale, stating:

> Under this final rule, it will be significantly more difficult for an individual to use a false name or provide fraudulent documents to obtain an identification that can be used for purposes of boarding a commercial airplane. Therefore, the final rule makes it less likely that a terrorist could circumvent watch-list screening processes and security procedures (as upgraded or developed post-9/11) and board a commercial airplane.[151]

However, in the final rule, the Department of Homeland Security includes an exception that completely undercuts the supposed security rationale for the creation of this national identification system. In the final rule, the Department of Homeland Security allows individuals to show their foreign passport in place of REAL ID card or other US-issued identification document.[152] Criminals who do not wish to go through the cumbersome REAL ID process could merely go to any number of foreign countries and obtain (whether legally or illegally) a passport that would "prove" their identity as a "trusted" individual, one whose name is not on any watch lists.

All of the 9/11 hijackers could have boarded commercial flights or entered federal buildings under the REAL ID scheme because each hijacker had a foreign passport, according to the 9/11 Commission Report.[153] In fact, "potential hijackers [were told] to acquire new 'clean' passports in their home countries before applying for a U.S. visa. This was to avoid raising suspicion about previous travel to countries where al Qaeda operated," said the Commission.[154] The 9/11 Commission in 2004 detailed the problem with the national security rationale that DHS continues to use in 2008.

Also, note that the Department of Homeland Security says in the final rule that it will be "significantly more difficult," but not impossible, "for an individual to use a false name or provide fraudulent documents to obtain an identification." This is the reason that any national identification system is fundamentally flawed: Individuals are told to "trust" the national ID card, but it is still possible to create a fake card, so one cannot rely on the national identification system to "prove" an individual is who she says. Contrary to the Department of Homeland Security's claims, this system harms our national security by creating another "trusted" path for criminals to exploit.

V. STATES OPPOSE NATIONAL ID SYSTEM

Since the passage of the REAL ID Act in 2005, a number of States have passed legislation rejecting the national identification system. On January 18, Montana governor Brian Schweitzer wrote to the governors of 17 States asking them to join him in rejecting the REAL ID system.[155] "Today, I am asking you to join with me in resisting the DHS coercion to comply with the provisions of REAL ID," Gov. Schweitzer wrote. "I would like us to speak with one, unified voice and demand the Congress step in and fix this mess."[156]

Four states (Maine, Montana, New Hampshire and South Carolina) have expressly rejected the system and none asked for an extension. After much posturing, DHS gave extensions to all States, even though some said they would never implement REAL ID, because their legislatures have passed laws banning the national identification system.[157]

In the final regulations released in January, the Department of Homeland Security set an extension request deadline of March 31, 2008.[158] By that date, all 56 States and U.S. territories were required to ask the agency for an extension that would allow their licenses and ID cards to remain "valid for federal purposes" past May 11, 2008 through the first extension period, until December 31, 2009.[159] For States that do ask for the initial extension, those States then have until October 11, 2009 to "file a request for an additional extension until no later than May 10, 2011, by submitting a Material Compliance Checklist demonstrating material compliance."[160]

The extensions were necessary because, even though May 11, 2008 is the statutory deadline for implementation of the REAL ID system, not one State is in compliance with the federal law creating a national identification system. In fact, 19 States have passed resolutions or laws rejecting the national ID program.

The Department of Homeland Security said it "made extensions available for states that needed additional time to come into compliance, or to complete

ongoing security measures," implying that states that received extensions had agreed to implement the REAL ID national identification system.[161] However, a number of states have said that these extensions do not constitute an agreement to implement this national ID scheme.

For example, California (one of the most populous states) sent a letter to the Department of Homeland Security on March 18, stating, "California's request for an extension is not a commitment to implement REAL ID."[162] New Hampshire said, "because our Legislature voted overwhelmingly in 2007 to pass a bill that prohibits our state from implementing the REAL ID Act in New Hampshire, we cannot authorize implementation of the REAL ID regulations."[163]

There are also ongoing concerns about Homeland Security's cost computation. In the final regulations, DHS claims to reduce the cost of implementation for the REAL ID national identification system to $9.9 billion, a significant drop from the draft regulations' estimate of $23.1 billion.[164] However, there are significant problems with the agency's assumptions.

The agency assumes that only 75 percent of U.S. residents will not apply for a REAL ID national identification card.[165] DHS states that the remaining 25 percent will either not enter federal buildings or board commercial flights, or the people will use $100 U.S. passports.[166] The agency also ignores, among other things, the cost of creating the national identification database (or "hub" network) linking 56 States and territories.

The Department of Homeland Security also believes that it can sweep aside the fact that REAL ID is an unfunded mandate by allocating $360 million to the States for REAL ID implementation. The agency said it will offer, "$80 million in dedicated REAL ID grants and another $280 million in general funding as part of the Homeland Security Grant Program," which funds security programs such as first responder services.[167] However, the number still pales next to the agency's "reduced" estimate of $9.9 billion.

Currently Congress is considering legislation to repeal REAL ID.[168] Sen. Patrick Leahy, who co-sponsored legislation to replace REAL ID with the negotiated rulemaking process originally enacted in the 2004 Intelligence Reform and Terrorist Prevention Act, criticized the final regulations. "The Bush administration's REAL ID program will not only lead to long lines at every DMV across the country, it will impose a massive unfunded mandate on State governments while offering absolutely no federal privacy protections to our citizens," Sen. Leahy said.[169] "It is unfortunate that instead of addressing the fundamental problems this law poses for the States, the Administration appears content merely to prolong a contentious and unproductive battle to force the States to comply."

VI. RECOMMENDATION: DECENTRALIZE IDENTIFICATION

The REAL ID national identification system would harm rather than protect privacy and security, and such a system would exacerbate the country's growing identity theft problem. It decreases security to have a centralized system of identification, one ID card for many purposes, as there will be a substantial amount of harm when the card is compromised.[170]

A system of decentralized identification reduces the risks associated with security breaches and the misuse of personal information. Technological innovation can enable the development of context-dependent identifiers. A decentralized approach to identification is consistent with our commonsense understanding of identification. If you are banking, you should have a bank account number. If go to the library, you should have a library card number. If you rent videos from a store, you should have a video rental store card number. Utility bills, telephone bills, insurance, the list goes on. These context-dependent usernames and passwords enable authentication without the risk of a universal identification system. That way, if one number is compromised, all of the numbers are not spoiled and identity thieves cannot access all of your accounts. All of your accounts can become compartmentalized, enhancing their security.[171]

Internet companies are already moving to develop systems of multiple identification in part because of concerns that were identified in a consumer privacy case brought to the Federal Trade Commission ("FTC") in 2001. In that matter, EPIC and 12 organizations submitted a complaint to the FTC, detailing serious privacy implications of Microsoft Windows XP and Microsoft Passport.[172] The complaint alleged that Microsoft "has engaged, and is engaging, in unfair and deceptive trade practices intended to profile, track, and monitor millions of Internet users," and that the company's collection and use of personal information violated Section 5 of the Federal Trade Commission Act.[173]

In August 2002, the FTC announced a settlement in its privacy enforcement action against Microsoft.[174] The settlement required that Microsoft establish a comprehensive information security program for Passport, and prohibited any misrepresentation of its practices regarding information collection and usage.

Since the FTC settlement of the EPIC complaint against Passport, industry groups have moved toward decentralized identity systems that are more robust, provide more security, and are better for privacy. Microsoft has developed an approach to identity management that allowed for multiple forms of online identification, and other companies, including open source developers, followed a similar approach.[175] There is a need to avoid single identifiers and to promote

multiple identification schemes, and that this approach is best not only for privacy but also for security.

The development of system for multiple identification, or "meta-identification" is widely favored by experts in the field. For example, Jim Harper, Director of Information Policy Studies at the Cato Institute, explains that the REAL ID Act does not add to the nation's security protections.[176] Instead, Harper advocates a diverse identification system. "A diverse, competitive identification and credentialing industry would be far better, and far more protective of liberty, than the uniform government-monopolized identification system on the advance today."[177]

VII. CONCLUSION

When Congress created the Department of Homeland Security, it made clear in the enabling legislation that the agency could not create a national ID system.[178] In September 2004, then-Department of Homeland Security Secretary Tom Ridge reiterated, "[t]he legislation that created the Department of Homeland Security was very specific on the question of a national ID card. They said there will be no national ID card."[179]

In an opinion column written by Secretary Chertoff after the publication of the final rule, he said, "embracing REAL ID" would mean it would be used to "cash a check, hire a baby sitter, board a plane or engage in countless other activities."[180] This is a description of a national identification system, which is illegal in the United States.

The final rule includes few protections for individual privacy and security in its massive national identification database. It harms national security by creating yet another "trusted" credential for criminals to exploit. The Department of Homeland Security has faced so many obstacles with the REAL ID system that the agency now plans an implementation deadline of 2017 – nine years later than the 2008 statutory deadline.[181] It is an unfunded mandate that would cost billions, with the burden ultimately being placed on the individual taxpayer.

Technical experts familiar with the challenges of privacy protection and identification presented the Department of Homeland Security with a variety of recommendations that would have minimized the risks of the REAL ID system. The DHS made some modifications, but left the essential system in place. As REAL ID currently stands, the costs are many and the benefits are few. Public opposition to implementation is understandable.

Appendix I

STATE LEGISLATION AGAINST REAL ID ACT

State Legislation Against REAL ID Act	
Alaska, SB 202 (April 11, 2008)*	Colorado, HJR 1047 (May 14, 2007)
South Dakota, SCR 7 (February 25, 2008)	Georgia, SB 5 (May 11, 2007)
Tennessee, SJR 0248 (June 14, 2007)	Hawaii, SCJ 31 (April 25, 2007)
South Carolina, S 449 (June 5, 2007)	North Dakota, SCR 4040 (April 20, 2007)
Nebraska, LR 28 (May 30, 2007)	Washington SB 5087 (April 18, 2007)
New Hampshire, HB 685 (May 24, 2007)	Montana, HB 287 (April 17, 2007)
Oklahoma, SB 464 (May 23, 2007)	Arkansas, SCR 22 (March 28, 2007)
Illinois, HJR 0027 (May 22, 2007)	Idaho: HJM 3 (March 12, 2007) HB 606 (April 9, 2008)
Missouri, HCR 20 (May 17, 2007)	Maine, SP 113 (January 25, 2007)
Nevada, AJR 6 (May 14, 2007)	
**Date passed*	Source: http://epic.org/privacy/id-cards/

Appendix II

EPIC EXPERT COMMENTS ON DRAFT REAL ID REGULATIONS

"EPIC and 24 Experts in Privacy and Technology, Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes (May 8, 2007)," available at http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

Signatories (affiliations are for identification only)

Steven Aftergood, Director of Project on Government Secrecy, Federation of American Scientists

Anita Allen, J.D., Ph.D., Henry R. Silverman Professor of Law and Professor of Philosophy, University of Pennsylvania Law School

Ann Bartow, Associate Professor of Law, University of South Carolina School of Law

Christine L. Borgman, Professor & Presidential Chair in Information Studies, University of California, Los Angeles

James Boyle, William Neal Reynolds Professor of Law, Duke University School of Law

David Chaum, Founder, DigiCash Inc.

Julie E. Cohen, Professor of Law, Georgetown University Law Center

Simon Davies, Director General, Privacy International

Dr. Whitfield Diffie, Chief Security Officer, Sun Microsystems

David Farber, Distinguished Career Professor of Computer Science and Public Policy, Carnegie Mellon University

Philip Friedman, Friedman Law Offices, PLLC

Deborah Hurley, Chair, EPIC Board of Advisors

Jerry Kang, Professor of Law, UCLA School of Law

Chris Larsen, CEO, Prosper Marketplace, Inc.

Gary Marx, Professor Emeritus, Massachusetts Institute of Technology

Mary Minow, LibraryLaw.com

Dr. Peter G. Neumann, Principal Scientist, SRI International Computer Science Lab

Dr. Deborah Peel, Founder, Patients Privacy Rights

Stephanie Perrin, Director of Integrity Policy, Service Canada

Anita Ramasastry, Associate Professor of Law, University of Washington School of Law

Dr. Bruce Schneier, Chief Technical Officer, BT Counterpane

Robert Ellis Smith, Publisher, Privacy Journal

Daniel J. Solove, Associate Professor of Law, George Washington University Law School

Frank M. Tuerkheimer, Professor of Law Emeritus, University of Wisconsin Law School

End Notes

[1] *See generally,* EPIC, National ID Cards and the REAL ID Act, http://www.epic.org/privacy/id_cards/.
[2] *See* EPIC AND PRIVACY INTERNATIONAL, PRIVACY AND HUMAN RIGHTS: AN INTERNATIONAL SURVEY OF PRIVACY LAWS AND PRACTICE 23-41 (EPIC 2006).
[3] *Id.* at 23-24.
[4] Dep't of Health, Educ. & Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens* 125-35 (MIT 1973) [hereinafter "HEW Report on Data Systems"], *available at* http://www.epic.org/privacy/hew1973report/.
[5] *See generally*, EPIC, Social Security Numbers, http://www.epic.org/privacy/ssn/.
[6] Soc. Sec. Admin., Soc. Sec. Number Task Force, *Report to the Commissioner* (May 1971).
[7] HEW Report on Data Systems at 125-35 (MIT 1973), *supra* note 4.
[8] Dep't of Justice, Fed. Advisory Comm. on False Identification, *The Criminal Use of False Identification* (Nov. 1976).
[9] Privacy Prot. Study Comm'n, *Personal Privacy in an Information Society* (July 1977) *available at* http://www.epic.org/privacy/ppsc1977report/.
[10] *Id.*
[11] Robert B. Cullen, *Administration Announcing Plan*, ASSOCIATED PRESS, July 30, 1981.
[12] Press Release, White House Office of the Press Secretary, The Health Security Act Of 1993: Health Care That's Always There (Sept. 22, 1993) *available at* http://www.clintonfoundation.org/legacy/092293-press-release-on-health-security-plan.htm.
[13] Illegal Immigration Reform and Immigrant Responsibility Act of 1996, Pub. L. No. 104-208, Div. C, Title III, § 309 (1996), *amended by* the Immigration and Naturalization Service Data Management Improvement Act of 2000, Pub. L. No. 106-215, 114 Stat. 337 (2000).
[14] Summer Lemon, *Ellison offers free software for national ID card*, IDG.NET, Sept. 25, 2001, *available at* http://archives.cnn.com/2001/TECH/industry/09/25/ellison.software.idg/.
[15] Declan McCullagh, *Oracle Keeps Pushing ID Card*, WIRED NEWS, Nov. 17, 2001, *available at* http://www.wired.com/news/politics/0,1283,48482,00.html.
[16] Homeland Security Act of 2002 § 554, 6 U.S.C. § 554 (2004).
[17] *Id.*
[18] Such proposals include the Western Hemisphere Travel Initiative PASSCard and "enhanced" driver's licenses with citizenship designations. *See* EPIC, *Comments on Docket No. USCBP–2007–0061: Proposed Rule: Documents Required for Travelers Departing From or Arriving in the United States From Within the Western Hemisphere* (Aug. 1, 2007), *available at* http://www.epic.org/privacy/rfid/whti_080107.pdf; EPIC, Spotlight on Surveillance, *Proposed 'Enhanced' Licenses Are Costly to Security and Privacy*, http://epic.org/privacy/surveillance/spotlight/0907/.
[19] Pub. L. No. 109-13, 119 Stat. 231 (2005) [hereinafter "REAL ID Act"].
[20] Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration (Apr. 12, 2005), *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=PressReleases.Detail&Affiliation=C&PressRelease_id=b456811f-b97a-4d4c-8503-cacbaaa649ca&Month=4&Year=2005.
[21] *Id.*
[22] EPIC, "National ID at the Crossroads: The Future of Privacy in America," (June 6, 2005) (a public conference on "The technology of identification; Lessons of RFID passports; and An organized response to REAL ID"), http://epic.org/events/id/.
[23] Dep't of Homeland Sec., *Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 72 Fed. Reg. 10,819 (Mar. 9, 2007) [hereinafter "REAL ID Draft Regulations"], *available at* http://edocket.access.gpo.gov/2007/07-1009.htm; *see generally*, EPIC, Spotlight on Surveillance,

Federal REAL ID Proposal Threatens Privacy and Security (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307; Anita Ramasastry, *Why the New Department of Homeland Security REAL ID Act Regulations are Unrealistic: Risks of Privacy and Security Violations and Identity Theft Remain, and Burdens on the States Are Too Severe*, Findlaw, Apr. 6, 2007, *available at* http://writ.news.findlaw.com/ramasastry/20070406.html.

[24] EPIC and 24 Experts in Privacy and Technology, *Comments on DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) [hereinafter "EPIC Expert Comments on Draft Regulations"], *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf. See Appendix II.

[25] Privacy Coalition, "Speak Out Against REAL ID," http://privacycoalition.org/stoprealid/.

[26] Though the Department of Homeland Security announced the final rule on Jan. 11, 2008, it was not published in the Federal Register until 18 days later. Dep't of Homeland Sec., *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271 (Jan. 29, 2008) [hereinafter "REAL Final Rule"], *available at* http://edocket.access.gpo.gov/2008/08-140.htm.

[27] *See* discussion in *Section IX. Recent Developments: States Continue Rebellion Against National ID System*.

[28] *Id.*; *Also*, Press Release, S. Comm. on Homeland Sec. & Governmental Affairs, Twelve Senators Urge Frist To Keep Real ID Act Off Supplemental Appropriations Bill Sweeping Proposal Needs Deliberate Consideration *supra* note 20.

[29] *See* ACLU, Real Nightmare: What's Wrong with REAL ID, http://realnightmare.org/; and Identity Project, http://www.papersplease.org/wp/.

[30] Security expert Bruce Schneier has detailed a number of problems with REAL ID in publications and Congressional testimony. *See* CRYPTO-GRAM newsletter, http://www.schneier.com/crypto-gram-back.html.

[31] Michael Chertoff, Sec'y, Dep't of Homeland Security, *Remarks at a Press Conference on REAL ID*, Jan. 11, 2008 [hereinafter "Chertoff Remarks on Final Rule"], *available at* http://www.dhs.gov/xnews/speeches/sp_1200320940276.shtm.

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] 5 U.S.C. § 552a (1974).

[36] EPIC Expert Comments on Draft Regulations at 3, *supra* note 24.

[37] *Id.* at 4, *quoting* Richard C. Barth, Assistant Sec'y for Policy Dev., Dep't of Homeland Sec., *Testimony at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards Before the Subcomm. on Oversight of Gov't Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs,* 110th Cong. (Mar. 26, 2007), *available at* http://hsgac.senate.gov/public/_files/Testimonybarth.pdf.

[38] *See e.g.*, Comm'n on Fed. Election Reform (aka "Carter-Baker Commission"), *Building Confidence in U.S. Elections* (Sept. 2005), *available at* http://www.american.edu/ia/cfer/report/full_report.pdf.

[39] REAL Final Rule at 5288, *supra* note 26.

[40] *Id.* at 5319. In March 2007, a Homeland Security official testified to Congress that "widespread acceptance" of REAL ID would affect employment and voting. *See* Richard C. Barth, *supra* note 37.

[41] Chertoff Remarks on Final Rule, *supra* note 31.

[42] REAL Final Rule at 5329, *supra* note 26.

[43] Ryan Singel, *Montana Governor Foments Real ID Rebellion*, WIRED, Jan. 18, 2008, http://blog.wired.com/27bstroke6/2008/01/montana-governo.html.

[44] *Id.*

[45] Dep't of State, Passport Fees, http://travel.State.gov/passport/get/fees/fees_837.html.
[46] REAL Final Rule at 5322, *supra* note 26.
[47] REAL ID Act at §§ 202(c)(1), 202(c)(2)(B), *supra* note 19.
[48] REAL Final Rule at 5333, *supra* note 26.
[49] *Id.* at 5277.
[50] EPIC Expert Comments on Draft Regulations at 13, *supra* note 24.
[51] *Id.* at 14.
[52] *Id.* at 53-54.
[53] REAL Final Rule at 5334, *supra* note 26.
[54] *Id.* at 5298.
[55] *Id.* at 5334.
[56] REAL ID Draft Regulations at 10,822, *supra* note 23.
[57] REAL Final Rule at 5315, *supra* note 26.
[58] *Id.* at 5298.
[59] EPIC Expert Comments on Draft Regulations at 14-17, *supra* note 24.
[60] REAL Final Rule at 5296, 5334, *supra* note 26; Electronic Verification of Vital Events ("EVVE") is also called Electronic Verification of Vital Event Records ("EVVER") in some federal documents.
[61] Nat'l Governors Ass'n, et. al, *The REAL ID Act: National Impact Analysis* (Sept. 19, 2006), *available at* http://www.nga.org/Files/pdf/0609REALID.PDF.
[62] *See* EPIC, Social Security Numbers, *supra* note 5 *and* EPIC, Spotlight on Surveillance, *Proposed 'Enhanced' Licenses Are Costly to Security and Privacy*, http://epic.org/privacy/surveillance/spotlight/0907/.
[63] Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's Numident File, A-08-06-26100* 6 (Dec. 18, 2006), *available at* http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.
[64] *Id.* at Appendix C-2.
[65] Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays, Rept. No. I-97-08* (Sept. 1997), *available at* http://www.usdoj.gov/oig/reports/INS/e9708/index.htm; *Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays, Rept. No. I-2002-006* (Apr. 2002), *available at* http://www.usdoj.gov/oig/reports/INS/e0206/index.htm/; and *Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration, Rept. No. I-2003-001* (Nov. 2002), *available at* http://www.usdoj.gov/oig/reports/INS/e0301/final.pdf.
[66] *AFL-CIO v. Chertoff,* No. C 07-04472 CRB (N.D. Cal. 2007), *available at* http://www.aclu.org/images/asset_upload_file505_32133.pdf.
[67] REAL Final Rule at 5297, *supra* note 26.
[68] EPIC Expert Comments on Draft Regulations at 15-16, *supra* note 24, *citing* REAL ID Draft Regulations at 10,833, *supra* note 23.
[69] REAL Final Rule at 5275-5276, *supra* note 26.
[70] *Id.* at 5297.
[71] "As of October 2007 [the most recent data available], the following vital records offices are online with EVVE: Arkansas, Hawaii, Iowa, Kentucky, Minnesota, Mississippi, Missouri, Montana, North Dakota, South Dakota and Utah." Nat'l Ass'n for Public Health Statistics & Info. Systems, *Electronic Verification of Vital Events (EVVE)*, http://www.naphsis.org/index.asp?bid=1036.
[72] REAL ID Draft Regulations at 10,831, *supra* note 23.
[73] REAL Final Rule at 5297, *supra* note 26.
[74] REAL ID Draft Regulations at 10,832, *supra* note 23.
[75] REAL Final Rule at 5297, *supra* note 26.
[76] *Id.*
[77] EPIC Expert Comments on Draft Regulations at 16-17, *supra* note 24.

[78] REAL Final Rule at 5277, *supra* note 26.
[79] REAL Final Rule at 5333, *supra* note 26.
[80] *Id.* at 5277.
[81] Dep't of Homeland Sec., *Regulatory Evaluation; Notice of Proposed Rulemaking; REAL ID; 6 CFR Part 37; RIN: 1061-AA37; Docket No. DHS-2006-0030* at 122 (Feb. 28, 2007) [hereinafter "DHS's Regulatory Evaluation of Draft REAL ID Regulations"], *available at* http://www.epic.org/privacy/id_cards/reg_eval_draftregs.pdf.
[82] REAL Final Rule at 5338, *supra* note 26.
[83] Gov't Accountability Office, *Social Security Administration: Actions Taken to Strengthen Procedures for Issuing Social Security Numbers to Noncitizens, but Some Weaknesses Remain*, GAO-04-12 (Oct. 2003), *available at* http://www.gao.gov/cgi-bin/getrpt?GAO-04-12.
[84] *Id.* at 19.
[85] EPIC Expert Comments on Draft Regulations at 17, *supra* note 24.
[86] REAL ID Draft Regulations at 10,825, *supra* note 23.
[87] Sen. Joseph Lieberman, *Statement at a Hearing on Understanding the Realities of REAL ID: A Review of Efforts to Secure Drivers' Licenses and Identification Cards Before the Subcomm. on Oversight of Gov't Management, the Federal Workforce & the District of Columbia, S. Comm. on Homeland Sec. & Governmental Affairs*, 110th Cong. (Mar. 26, 2007).
[88] EPIC Expert Comments on Draft Regulations at 6-12, *supra* note 24.
[89] Office of Mgmt. & Budget, *Privacy Act Implementation: Guidelines and Responsibilities*, 40 Fed. Reg. 28,948, 28,951 (July 9, 1975), *available at* http://www.whitehouse.gov/omb/inforeg/implementation_guidelines.pdf.
[90] *Id.*
[91] Privacy Office, Dep't of Homeland Sec., *Privacy Policy Guidance Memorandum* 2 (Jan. 19, 2007), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf.
[92] *Id.* at 1.
[93] REAL Final Rule at 5284-5284, *supra* note 26.
[94] EPIC Expert Comments on Draft Regulations at 17-28, *supra* note 24.
[95] REAL ID Act at § 202(b), *supra* note 19.
[96] REAL Final Rule at 5336, *supra* note 26.
[97] Dep't of Homeland Sec., Data Privacy & Integrity Advisory Committee, "The Use of RFID for Human Identity Verification," Report No. 2006-02 (Adopted Dec. 6, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf. *See also,* Wilson Dizard, *DHS privacy office slams RFID technology,* COMPUTERWORLD, May 7, 2006, *available at* http://www.gcn.com/online/vol1_no1/40808-1.html.
[98] *Id.* at 5292.
[99] Dep't of Homeland Sec. Privacy Office, *Privacy Impact Assessment for the REAL ID Act* 16 (Mar. 1, 2007), *available at* http://www.epic.org/privacy/id_cards/pia_030107.pdf.
[100] EPIC Expert Comments on Draft Regulations at 21-23, *supra* note 24.
[101] *Id.*
[102] *Id.* at 17-18.
[103] REAL Final Rule at 5292, *supra* note 26.
[104] EPIC Expert Comments on Draft Regulations at 19, *supra* note 24.
[105] REAL ID Act at § 202(b)(8), *supra* note 19.
[106] REAL Final Rule at 5275, 5291, *supra* note 26.
[107] EPIC Expert Comments on Draft Regulations at 31-33, *supra* note 24.
[108] Melissa Ngo, Dir., Identification & Surveillance Project, EPIC, *Prepared Testimony and Statement for the Record at a Meeting on "REAL ID Rulemaking" Before the Data Privacy & Integrity Advisory Comm., Dep't of Homeland Sec.* (Mar. 21, 2007), *available at* http://www.epic.org/privacy/id_cards/ngo_test_032107.pdf.

[109] Press Release, EPIC, After Long Delay, Homeland Security Department Announces Regulations For Deeply Flawed National ID System (Jan. 11, 2008), *available a*t http://epic.org/press/011108.html.
[110] *Five indicted in identity theft scheme*, BALTIMORE SUN, Jan. 11, 2008.
[111] Fed. Trade Comm'n, *2006 Identity Theft Survey Report* 3 (Nov. 2007), *available at* http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.
[112] *Id.* at 5.
[113] *Id.* at 6.
[114] Privacy Rights Clearinghouse, A Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.
[115] *Id.*
[116] *Id.*
[117] EPIC Expert Comments on Draft Regulations at 50, *supra* note 24.
[118] Press Release, Dep't of Justice, Former Department of Commerce Agent Indicted For Making a False Statement and Exceeding Authorized Access To a Government Database (Sept. 19, 2007), *available at* http://www.usdoj.gov/usao/can/press/2007/2007_09_19_robinson.indicted.press.html.
[119] *Id*.
[120] Michael Kiefer, *Officer Admits to Tampering; Databases Used to Check on Women*, ARIZONA REPUBLIC, April 6, 2006, at 3B. More insider and outsider abuses are detailed in our May 2007 comments. EPIC Expert Comments on Draft Regulations at 45, 50-51, *supra* note 24.
[121] Kevin Murphy, *Officer's Actions will Cost 25,000*, GAZETTEXTRA, Feb. 15, 2007, http://www.gazetteextra.com/mezera021507.asp.
[122] REAL Final Rule at 5338, *supra* note 26.
[123] REAL ID Draft Regulations at 10,856, *supra* note 23.
[124] EPIC Expert Comments on Draft Regulations at 51, *supra* note 24.
[125] *Id*.
[126] REAL ID Draft Regulations at 10,856, *supra* note 23.
[127] 49 C.F.R. 1572.103(a).
[128] *Id.* at 1572.103(b)(2)(iii).
[129] EPIC Expert Comments on Draft Regulations at 52, *supra* note 24.
[130] REAL Final Rule at 5338, *supra* note 26.
[131] EPIC Expert Comments on Draft Regulations at 46-50, *supra* note 24.
[132] REAL ID Act at § 202(b)(6), *supra* note 19.
[133] Violence Against Women & Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, § 827, 119 Stat. 2960, 3066 (2005) [hereinafter "VAWA"].
[134] *Id*.
[135] REAL Final Rule at 5335, *supra* note 26.
[136] *Id.*
[137] *Id.* at 5336.
[138] *Id.* at 5333.
[139] *Id*. at 5302.
[140] REAL Final Rule at 5337, *supra* note 26.
[141] *Id*. at 5300.
[142] *Id.* at 5333.
[143] *Id.*
[144] *Id.* at 5335-36.
[145] REAL Final Rule at 5337, *supra* note 26.
[146] *Id.*
[147] Chertoff Remarks on Final Rule, *supra* note 31.
[148] EPIC Expert Comments on Draft Regulations at 33-39, *supra* note 24.
[149] *Id*.

[150] DHS's Regulatory Evaluation of Draft REAL ID Regulations at 127, *supra* note 81.
[151] REAL Final Rule at 5285, *supra* note 26.
[152] *Id*. at 5333.
[153] Nat'l Comm'n on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (July 2004), *available at* http://govinfo.library.unt.edu/911/report/index.htm.
[154] *Id*. at 236.
[155] Letter from Montana Governor Brian Schweitzer to 17 States (Jan. 18, 2008), *available at* http://governor.mt.gov/brian/RealID_080118.pdf.
[156] *Id*.
[157] Press Release, Dep't of Homeland Sec., All Jurisdictions Meet Initial REAL ID Requirements (Apr. 2, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1207167055742.shtm.
[158] REAL Final Rule at 5339, *supra* note 26.
[159] *Id*.
[160] *Id*.
[161] Press Release, Dep't of Homeland Sec., Most Jurisdictions Meet Initial REAL ID Requirements (Apr. 1, 2008), *available at* http://www.dhs.gov/xnews/releases/pr_1207079095443.shtm.
[162] Letter from George Valverde, Dir., Calif. Dep't of Motor Vehicles, to Michael Chertoff, Sec'y, Dep't of Homeland Sec., Mar. 18, 2008, *available at* http://epic.org/privacy/id-cards/calif_dhs_031808.pdf.
[163] Letter from Earl M. Sweeney, Assistant Comm'r, N.H. Dep't of Safety, to Stewart Baker, Assistant Sec'y for Policy, Dep't of Homeland Sec. Mar. 26, 2008, *available at* http://epic.org/privacy/id-cards/nj_dhs_032608.pdf.
[164] REAL Final Rule at 5324, *supra* note 26; EPIC Expert Comments on Draft Regulations at 33-39, 41-46, *supra* note 24.
[165] REAL Final Rule at 5322, *supra* note 26.
[166] *Id*.
[167] Press Release, Dep't of Homeland Sec., DHS Releases REAL ID Regulation, Jan. 11, 2008, *available at* http://www.dhs.gov/xnews/releases/pr_1200065427422.shtm.
[168] S. 717, *A bill to repeal title II of the REAL ID Act of 2005, to restore section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004, which provides States additional regulatory flexibility and funding authorization to more rapidly produce tamper- and counterfeit-resistant driver's licenses, and to protect privacy and civil liberties by providing interested stakeholders on a negotiated rulemaking with guidance to achieve improved 21st century licenses to improve national security*, 110th Cong. (2008); H.R. 1117, *A bill to repeal title II of the REAL ID Act of 2005, to reinstitute section 7212 of the Intelligence Reform and Terrorism Prevention Act of 2004, which provides States additional regulatory flexibility and funding authorization to more rapidly produce tamper- and counterfeit-resistant driver's licenses and to protect privacy and civil liberties by providing interested stakeholders on a negotiated rulemaking with guidance to achieve improved 21st century licenses to improve national security*, 110th Cong. (2008).
[169] Press Release, Office of Sen. Patrick Leahy, Reaction of Sen. Patrick Leahy (D-Vt.) on Release of the Final REAL ID Regulations by the U.S. Department of Homeland Security (Jan. 11, 2008), *available at* http://leahy.senate.gov/press/200801/011108a.html.
[170] For more discussion of identifiers, *see* EPIC, *Comments to the Federal Trade Commission on Private Sector Use of Social Security Numbers: Topics For Comment* (Sept. 5, 2007), *available a*t http://www.epic.org/privacy/ssn/ftc_ssn_090507.pdf.
[171] *Id*.
[172] In the Matter of Microsoft Corporation File No. 012 3240, Docket No. C-4069 (Aug. 2002), *available at* http://www.ftc.gov/os/caselist/0123240/0123240.shtm.
[173] *Id*. at 1.
[174] Fed. Trade Comm'n, *Microsoft Settles FTC Charges Alleging False Security and Privacy Promises* (Aug. 2002) ("The proposed consent order prohibits any misrepresentation of information practices in connection with Passport and other similar services. It also requires Microsoft to

implement and maintain a comprehensive information security program. In addition, Microsoft must have its security program certified as meeting or exceeding the standards in the consent order by an independent professional every two years."), *available at* http://www.ftc.gov/opa/2002/08/microsoft.shtm.

[175] Kim Cameron, *The Laws of Identity*, IDENTITY WEBLOG, Dec. 9, 2004, http://www.identityblog.com/stories/2004/12/09/thelaws.html; Windows CardSPace, http://cardspace.netfx3.com/; OpenCard, http://www.opencard.org/.

[176] JIM HARPER, IDENTITY CRISIS: HOW IDENTIFICATION IS OVERUSED AND MISUNDERSTOOD (Cato Institute 2006).

[177] *Id*. at 5.

[178] Pub. L. No. 107-296, 116 Stat. 2135 (2002).

[179] Tom Ridge, Sec'y, Dep't of Homeland Sec., *Address at the Center for Transatlantic Relations at Johns Hopkins University: "Transatlantic Homeland Security Conference,"* Sept. 13, 2004, *available at* http://www.dhs.gov/xnews/speeches/speech_0206.shtm.

[180] Michael Chertoff, *National ID security*, SACRAMENTO BEE, Jan. 16, 2008, *available at* http://www.sacbee.com/110/story/636479.html.

[181] REAL Final Rule at 5333, *supra* note 26.

From: Edward Hasbrouck
Sent: Mon, 9 Jan 2017 16:26:14 -0500
To: TSAPRA;DHS.InfoQuality
Subject: Comments on TSA-2013-0001-0075 and petition for redress for information dissemination
Attachments: Attachment information, IDP-form-415-9JAN2017.pdf

Attached please find comments of the Identity Project and the Cyber Privacy Project the Cyber Privacy Project in response to the notice and request for comments, "Intent To Request Approval From OMB of One New Public Collection of Information: Certification of Identity Form (TSA Form 415)", docket number TSA-2013-0001-0075, FR Doc. 2016-26958, published at 81 Federal Register 78624-78625 (November 8, 2016).

These comments also include and constitute a complaint and request for redress regarding the accuracy of information disseminated by the TSA in this notice, pursuant to the Information Quality Act.

This item is incorrectly labeled as closed to comment on Regulations.gov, so we are unable to submit comments or obtain confirmation of comment submission through the Regulations.gov website. Please reply to confirm your receipt and docketing of these comments and this complaint.

Sincerely,

Edward Hasbrouck

Edward Hasbrouck
(b)(6)
<http://hasbrouck.org>
1130 Treat Ave., San Francisco, CA 94110, USA
(b)(6)

consultant to The Identity Project (IDP),
a program of the First Amendment Project
<http://www.papersplease.org>

"Congress shall make no law ... abridging ... the right of the people peaceably to assemble" (U.S. Constitution, Amendment 1)

"Everyone has the right to freedom of movement and residence within the borders of each state. Everyone has the right to leave any country, including his own, and to return to his country." (Universal Declaration of Human Rights, Article 13)

"Liberty of movement is an indispensable condition for the free development of a person." (United Nations Human Rights Committee, General Comment No. 27)

Before

U.S. CUSTOMS AND BORDER PROTECTION
DEPARTMENT OF HOMELAND SECURITY

Washington, DC 20229

Intent To Request Approval From OMB of One New [sic] Public Collection of Information: Certification of Identity Form (TSA Form 415); TSA-2013-0001-0075, FR Doc. 2016-26958	**COMMENTS OF THE IDENTITY PROJECT (IDP) AND THE CYBER PRIVACY PROJECT (CPP)**

The Identity Project (IDP)

<http://www.PapersPlease.org>

Cyber Privacy Project (CPP)

<http://www.cyberprivacyproject.org>

January 9, 2017

CONTENTS

I. INTRODUCTION

The Identity Project (IDP) and the Cyber Privacy Project (CPP) submit these comments in response to the notice and request for comments, "Intent To Request Approval From OMB of One New Public Collection of Information: Certification of Identity Form (TSA Form 415)", docket number TSA-2013-0001-0075, FR Doc. 2016-26958, published at 81 *Federal Register* 78624-78625 (November 8, 2016).

The notice fails to satisfy the requirements of the Administrative Procedure Act (APA), the Paperwork Reduction Act (PRA), and the Privacy Act. The notice miscategorizes the proposal, fails to provide adequate or accurate notice to the public, and includes materially false statements about the proposal and the history and status of TSA Form 415.

The notice attempts to use the PRA procedures for approval of a form to effect a sweeping, highly controversial, substantive change in the scope of authority over air travelers claimed and exercised by the TSA. Even if such a change were authorized by a valid statute, it would require a different procedure: notice-and-comment rulemaking by the TSA pursuant to the APA. The significance of these procedural violations is heightened because the proposal implicates the ability of individuals to exercise their right – pursuant to Federal statutes, the U.S. Constitution, and international human rights treaties – to travel by air by common carrier.

The proposal for approval of TSA Form 415 and of this information collection by OMB should be withdrawn. The TSA should cease and desist from its years-old and continuing unlawful use of Form 415, and the additional associated verbal information collection, without the required OMB approval. If this proposal is submitted to OMB, it should be rejected as procedurally, substantively, and legally deficient and unjustified, and as a violation of the

fundamental statutory, Constitutional, and human rights of air travelers. If the TSA believes such a proposal is warranted, it should propose it though APA notice-and-comment rulemaking.

II. ABOUT THE COMMENTERS

A. The Identity Project (PapersPlease.org)

The Identity Project (IDP), provides advice, assistance, publicity, and legal defense to those who find their rights infringed, or their legitimate activities curtailed, by demands for identification, and builds public awareness about the effects of ID requirements on fundamental rights. IDP is a program of the First Amendment Project, a nonprofit organization providing legal and educational resources dedicated to protecting and promoting First Amendment rights.

B. The Cyber Privacy Project

The Cyber Privacy Project (CPP) is a non-partisan organization focusing on governmental intrusions against Fourth and Fifth Amendment rights of privacy, particularly in government databanks and national identification schemes for voting, travel, and work, and on medical confidentiality and patient consent.

III. THIS PROPOSAL IMPLICATES FREEDOM OF MOVEMENT, A STATUTORY, CONSTITUTIONAL, AND INTERNATIONALLY RECOGNIZED HUMAN RIGHT.

Freedom of movement ("the right of the people... peaceably to assemble") is recognized by the First Amendment to the U.S. Constitution.

The right of U.S. citizens to travel between states is among the “privileges and immunities” protected by Article IV of the U.S. Constitution, and is a “liberty” protected by the

due process requirements of the 5th and 14th Amendments. “The original conception of the travel right is explicitly stated in Article IV of the Articles of Confederation and remains in force in the parallel article of the U.S. Constitution. Travel embodies a broadly based personal, political, and economic right that encompasses all modes of transportation and movement.”[1]

The right to travel is also recognized in Article 12 (freedom of movement) of the International Covenant on Civil and Political Rights (ICCPR), a treaty ratified by, and binding on, the U.S. In addition, Article 17 of the ICCPR recognizes a right to protection against "arbitrary or unlawful interference with … privacy."

The TSA, along with all other executive agencies, has been ordered by the President to consider human rights treaties including the ICCPR in performing its functions including rulemaking: Executive Order 13107, “Implementation of Human Rights Treaties,” directs all executive departments and agencies to “maintain a current awareness of United States international human rights obligations that are relevant to their functions and... perform such functions so as to respect and implement those obligations fully.”

In addition to the general Constitutional right to travel, there is an explicit mode-specific Federal statutory right to travel by air. “The public right of freedom of transit through the navigable airspace” is guaranteed by the Airline Deregulation Act of 1978, codified at 49 USC § 40101, 40103. The same statute expressly requires that the Administrator of the TSA (exercising powers described in the statute as those of the Administrator of the FAA, but reassigned to the TSA as part of the creation of the TSA and the Department of Homeland Security), “shall consider” this right in carrying out agency functions, which include rulemaking.

---

1 Richard Sobel, The Right To Travel And Privacy: Intersecting Fundamental Freedoms, 30 J. Marshall J. Info. Tech. & Privacy L. 639, 640 (2014) <http://repository.jmls.edu/jitpl/vol30/iss4/1>.

It is essential to keep these rights in mind in assessing the proposed (and in fact, as discussed further below, longstanding and ongoing) information collection from travelers. To the extent that responding to this information collection (or providing responses that the TSA or its contractors deem acceptable) is made a condition of the exercise of the right to travel by common carrier, it is a condition on the exercise of a fundamental statutory, Constitutional, and international treaty right, and therefore subject to strict scrutiny.[2]

IV. THE NOTICE DOES NOT SATISFY THE REQUIREMENTS OF THE PAPERWORK REDUCTION ACT FOR APPROVAL OF A COLLECTION OF INFORMATION FROM MEMBERS OF THE PUBLIC.

Instead of providing actual notice of what the agency has done, is doing, and proposes to do, and how concerned members of the public can obtain more information, the notice concerning this proposed information collection published in the *Federal Register* contains materially false statements concerning the proposal and the agency's actions.

These material misstatements deprive the public of meaningful notice of what has actually happened and is happening, and of the opportunity to provide informed comment on the agency's past, present, and proposed future actions.

In addition, to the extent that – for whatever reason – those promulgating the notice genuinely believed these falsehoods, they were ignorant of essential and material elements of the administrative and factual record necessary for non-arbitrary agency decision-making.

2 This is merely a summary of some of the fundamental rights implicated by air travel by common carrier. As discussed further below, this proceeding is a request for approval of a form, not a proposal for regulations to require air travelers to present, possess, or be eligible to acquire acceptable government-issued ID credentials, or to identify themselves. We reserve the right to submit more detailed comments concerning the right to travel, the standard of review for conditions or restrictions on the exercise of this right, and the effect on this right of ID requirements for common carrier air travel if the TSA proposes rules to impose such a requirement.

A materially false notice does not satisfy the notice requirements of the PRA. A decision by agency officials ignorant of these facts would be arbitrary and capricious.

In addition, each of the false statements in the notice discussed below constitutes a violation of the "Information Quality Act" (IQA), Section 515 of the Consolidated Appropriations Act, 2001, Public Law 106–554, and the guidelines for implementation of this statute promulgated by OMB and the Department of Homeland Security (DHS).[3]

These comments constitute a "complaint[] … regarding the accuracy of information disseminated by" the TSA. In accordance with the IQA, we request that this complaint be included in reporting by the TSA and DHS to OMB of "the number and nature of complaints received by the agency regarding the accuracy of information disseminated by the agency."

A. The TSA does not currently require travelers to provide ID documents to fly. Such a new requirement is outside the scope of OMB authority to approve a collection of information, and requires TSA rulemaking pursuant to the APA.

According to the notice in the *Federal Register*:

> TSA requires individuals to provide an acceptable verifying identity document in order to proceed through security screening, enter the sterile area of the airport, or board a commercial aircraft.

In fact, the TSA does not require, and the law does not authorize the TSA to require, that would-be travelers provide any verifying identity documents. According to longstanding practice, people who do not provide any verifying identity document travel by air every day –

3 See OMB Agency Information Quality Guidelines, <https://www.whitehouse.gov/omb/_inforeg_agency_info_quality_links>; DHS Information Quality Standards, <https://www.dhs.gov/information-quality-standards>; and TSA Information Quality Standards, <https://www.tsa.gov/information-quality-standards>. Since the TSA has not responded to informal requests for correction of the notice, petitions for correction of the inaccurate information in the notice are being prepared for submission to DHS.

typically after being required to complete and sign TSA Form 415 and answer questions about what information is contained in the file about them obtained by the TSA from Accurint.[4]

The TSA's current policy permitting people to fly without ID if they submit to more intrusive search was described as follows by the 9th Circuit Court of Appeals in *Gilmore v. Gonzales*[5], based on review of TSA documents submitted *ex parte* and under seal:

> The identification policy requires airline passengers to present identification to airline personnel before boarding or be subjected to a search that is more exacting than the routine search that passengers who present identification encounter.[6]
>
> The identification policy requires that airline passengers either present identification or be subjected to a more extensive search. The more extensive search is similar to searches that we have determined were reasonable and "consistent with a full recognition of appellant's constitutional right to travel."[7]

As discussed in more detail in Parts V and VI of these comments below, the TSA has provided, in response to our Freedom of Information Act request, only incomplete and badly munged portions of its records of how many people fly without ID every day.

But the first interim response to this request, containing images of redacted excerpts from the TSA "IVCC [ID Verification Call Center] Daily Summary" for May 6, 2014, is instructive.[8]

On that date, 175 people were reported to the IVCC as having sought to proceed through TSA checkpoints without initially presenting ID that the checkpoint staff found acceptable.

---

4 See the more detailed discussion of these ongoing practices below in Part V of these comments.

5 435 F. 3d 1125 (9th Circuit 2006), cert. denied, 127 S. Ct. 929 (2007). Plaintiff-Appellant Gilmore is the founder of the Identity Project, one of the organizations submitting these comments.

6 *Gilmore v. Gonzales*, 435 F. 3d 1125 at 1141.

7 *Gilmore v. Gonzales*, 435 F. 3d 1125 at 1155.

8 This first interim response contained four images of "pages" of records pertaining to a single day, although we had requested all such records for all dates. We received this first interim response almost two years after submitting our FOIA request. Three and half years after we submitted this request, the TSA still has not completed its response. See request and all interim responses to date at <https://archive.org/details/TSOC-ID-Verification-Reports> and discussion of the status of this request in Note 22 below.

Of these 175 people, only three were denied access. The other 172 – more than 98% of those who sought to fly with no ID or with unacceptable ID – were allowed to do so.

In light of this current TSA policy and these facts, what the notice should say is:

> TSA *is proposing to require* individuals to have been issued a verifying identity document acceptable to the TSA, or reside in a state that the TSA has deemed compliant with the REAL-ID Act or that TSA has granted a discretionary extension of compliance with the REAL-ID Act, in order to proceed through security screening, enter the sterile area of the airport, or board a commercial aircraft.

When the substance of the proposal is stated accurately, the notice is fundamentally deficient. Approval for this change in requirements to travel (not a mere continuation of, or change in, an information collection) is being requested from the wrong agency, through the wrong procedure, and without an adequate basis.

A change in the requirements for air travel by common carrier – such as the proposed and entirely new requirement for each would-be traveler to provide the TSA with a verifying identity document or attest that they have been issued by some government agency with such a document or reside in a state that the DHS has deemed compliant with the REAL-ID Act or has granted an extension of compliance – could properly be initiated only through a Notice Of Proposed Rulemaking (NPRM) by the TSA in accordance with the procedural requirements of the APA.

If such an NPRM were promulgated for public comment, we and many others would object to the proposal. It exceeds the statutory authority of the TSA and is contrary to the statutory duty of the TSA to recognize the public right of transit by air, the Constitution, and U.S. obligations pursuant to international human rights treaties.

In addition, such a rule would not be related to any legitimate aviation security interest. According to the notice:

> TSA is updating the identity verification process for travelers who arrive at an airport security checkpoint without an acceptable verifying identity document... so that it is generally only available to travelers who certify that they—
>
> • Reside in or have been issued a driver’s license or state identification card by a state that is compliant with the REAL ID Act or a state that has been granted an extension by DHS; or
>
> • Have been issued another verifying identity document that TSA accepts.

It's important to understand just what the TSA is saying, and the import of the practice the notice describes. If the TSA were to promulgate such a rule, travelers would still be able to fly with no ID at all, just as they are today. This would still be true, as it is today, for individuals who have never been issued, or applied for, any government-issued ID. But it would only be permissible, under a rule such as the TSA is contemplating, for individuals without ID to fly if they reside in a state that issues ID acceptable to the TSA.

The essential idea is to discriminate between people who don't have or apply for state-issued ID cards, on the basis of how their states of residence treat those who do apply.

Variations in the practices followed by states in issuing driver's licenses and ID cards, or whether data about those driver's licenses and ID cards is shared with other states, provide no legitimate basis for differential treatment, on the basis of state of residence, of those individuals who do not have state-issued ID. Whatever claims the TSA might make about security benefits of these ID issuance procedures or their use as a basis for discrimination between holders of ID cards issued by different states, the state of residence of an individual who does not present ID bears no rational relationship to whether that individual poses a threat to aviation safety.

To put it another way, there is no reason to think that a person who has not chosen to apply for state ID as a resident of compliant state X posed less of a threat to aviation security than an individual who has not chosen to apply for state ID as a resident of noncompliant state Y.

Why, given the lack of any rational relationship of state of residence to aviation security, would the TSA discriminate between people who have not been issued with state ID on the basis of their state of residence, or on the basis of how that state treats people who, unlike these individuals, apply for or are issued with state ID?

The only apparent explanation for this otherwise perverse-seeming practice is that the TSA's real purpose in making this change is to coerce states to comply with the REAL-ID Act by punishing residents of states whose governments don't comply.

This is both an impermissible purpose and an impermissible practice. The Federal government has no authority to order states to enact legislation on matters within the jurisdiction of the states. The TSA has no authority to discriminate between residents of different states on the basis of the choices made by their state governments on matters within state jurisdiction.

We reserve the right to raise these and all other objections if and when such an NPRM is promulgated.

But this PRA notice in the *Federal Register* is not an NPRM. OMB is not authorized to approve substantive changes – or, for that matter, to approve any changes – in TSA regulations.

The only plausible interpretation of the false statement in the notice is to mislead OMB and the public, evade the requirement for public notice and comment, and use the innocuous-seeming device of a request for approval of an information collection to affect a

fundamental and profoundly controversial change in substantive TSA requirements and the rights of travelers.

The TSA does not have the authority to rule by decree, or to create a regulatory *fait accompli* by making new statements about what it seeks to require. Valid rulemaking requires the promulgation of rules, in accordance with the procedural requirements of the Administrative Procedure Act, Constitutional due process, and the procedural and substantive standards applicable pursuant to U.S.-ratified international human rights treaties.

If the TSA wants to "make it so" that each air traveler is required to provide an acceptable verifying identification document, or that air travel without ID be permitted only for residents of certain states specified by the DHS, the TSA must properly propose such a regulation, providing notice of what it proposes to require and of the basis for its claimed authority to require it.

Whether or not the TSA proceeds with such a rulemaking – which, to be clear, we don't think it should, and would oppose – OMB must reject this purported request for approval of an information collection as exceeding the scope of OMB authority, pursuant to the PRA, for approval of a collection of information.

B. TSA Form 415 and the associated verbal information collection are not new, and therefore cannot be approved by OMB as a “new” collection of information.

The notice describes TSA Form 415 and its use as "a new Information Collection Request (ICR) abstracted below that we will submit to the Office of Management and Budget (OMB) for approval in compliance with the Paperwork Reduction Act (PRA)."

But while TSA Form 415 has never been submitted to, nor approved by, OMB, neither the form, its use, nor the additional information collection associated with its use are "new". As chronicled in detail in Part V of these comments below, TSA Form 415 and its unnumbered predecessor form(s), and the associated verbal collection of information from travelers, have been in use since at least 2008.

Submission of a form or other proposed ICR to OMB for approval after it has been in use for more than eight years is not, by any plausible interpretation of the law, "in compliance with" the PRA, which requires OMB approval prior to the first use of a form or information collection.

The proposed submission to OMB should be described as a request for approval of an ICR that has been conducted unlawfully without OMB approval since at least 2008.

Given the extensive experience of the TSA and the public with this form and information collection, it would be arbitrary and capricious for OMB to approve it without review of its extensive track record. And proper notice and comment would include an invitation to members of the public to comment on their experiences with this form and information collection.

Without proper notice that this form and information collection have already been in use, potential commenters might think that they would have to speculate about its effects, and might not realize that there is an extensive agency record and body of public experience that could form the basis for better informed comments concerning the request for OMB approval.

In addition, potential commenters are likely to scrutinize the proposal more closely and critically if they know that the agency has been acting illegally for many years.

A new notice should be promulgated, properly describing this as a request for approval of an ICR that has been conducted unlawfully without OMB approval since at least 2008. A new opportunity for public comment should be provided following that notice.

C. Would-be commenters have been told that the comment deadline has passed, depriving them of the opportunity for comment required by the PRA.

The notice published in the *Federal Register* was posted "for comment" on Regulations.gov at <https://www.regulations.gov/document?D=TSA-2013-0001-0075>. But since the notice was first posted, that Web page has falsely described it as "Comment Period Closed", and has not included any comment submission button, link, or form.

We have been contacted by several members of the public who would have prepared and submitted comments, but did not do so, in reasonable reliance on Regulations.gov (which is read by far more people than the printed *Federal Register*) as an authoritative official source of information concerning notice and comment on proposed rules and agency actions.

We and other members of the public contacted the TSA staff person named in the notice, within days of the error appearing on Regulations.gov, to alert the agency that comments were not being accepted. The TSA has failed to have the false statement on Regulations.gov corrected.

TSA staff told us that, contrary to the plain language at the top of the page on Regulations.gov, comments were in fact open and would be accepted by email through January 9, 2017. But members of the public would have no reason to read further in the notice or attempt to submit comments by email once they read that the comment period had already closed.

Members of the public are entitled to rely on Regulations.gov for authoritative information about official Federal agency notices and opportunities for comment. Most members of the public, including many who have contacted us, assumed after consulting Regulations.gov that they were too late to submit comments. Most members of the public would not bother to prepare or try to submit comments by email after being told, through the official Federal government Web portal used for such purposes, that the comment period had already expired.

When the official Federal portal for comments is closed to comments throughout the "comment" period, there is no meaningful opportunity to comment. A new notice and opportunity for comment must be provided before any valid agency action can be taken.

D. No documentation concerning this request is available at Reginfo.gov, depriving members of the public of meaningful notice or opportunity to comment.

The notice claims that, “The ICR [Information Collection Review] documentation is available at http://www.reginfo.gov.” This claim is false: No information concerning this information collection has yet been submitted to OMB, and no information whatsoever concerning it is available at http://www.reginfo.gov, on any publicly-accessible Federal website, or from the TSA, even if it is specifically requested. The TSA contact designated in the notice has confirmed to us that no information other than that which was published in the *Federal Register* notice is available to would-be commenters or other members of the public.

It is critical for both the eventual reviewers of this request at OMB and any subsequent court reviewing this administrative action to be aware that the public has not been given actual

notice of, and an opportunity to comment on, any of these documents. They will only be submitted to OMB or posted at http://www.reginfo.gov *after* the close of public comments.

Despite our requests and diligent attempts to obtain, review, and comment on the allegedly supporting documentation referred to in the notice, it has been withheld from us.

A new opportunity for public comment must be offered after this documentation is made available to the public and public notice of its availability has been promulgated.

V. THE HISTORY OF TSA FORM 415 AND THE ASSOCIATED VERBAL COLLECTION OF INFORMATION FROM TRAVELERS BY THE TSA SHOWS A FAILURE TO COMPLY WITH THE PRA, APA, OR PRIVACY ACT.

In light of the false characterization of TSA Form 415 as "new" in the notice, and the notice that elides any discussion of the extensive experience of the TSA and the public with its use and with the additional associated information collection, we find ourselves obliged to supply a summary of the background facts that should have been included in the notice, and that need to be considered by OMB, commenters, and any subsequent reviewers.

The PRA requires approval by OMB and assignment of an OMB "control number" prior to the commencement of any systematic collection of information (whether by printed or electronic form or verbal questioning) from more than ten members of the public. The PRA also requires the inclusion of that OMB control number on the form itself, and requires other specified notices to each individual from whom information is to be collected.

The Privacy Act requires promulgation of a System Of Records Notice (SORN) describing what data is to be collected from what sources, and how it is to be used, and makes it a criminal offense to maintain a system of records about individuals without first doing so.

The APA requires public notice and an opportunity to comment on proposed regulations before they are finalized.

In 2008, when the TSA implemented the "procedures" involving the first version of Form 415, and the additional associated collection of information, the TSA did none of these things.

Rather than operate in accordance with the law, here's what the TSA actually did:

Following its standard operating procedure of rulemaking-by-press-release, the TSA announced changes to "Airport ID Requirements" on its website on June 5, 2008.[9] These were stated as "requirements", which would imply either statutory requirements or regulations adopted through notice-and-comment rulemaking pursuant to statutory authority. But neither the press release on the TSA website nor the subsequent TSA blog posts[10] about these new purported "requirements" cited to any current or proposed regulations or statutory authority.

Hundreds of public comments were posted in the TSA blog in response to these blog posts, and many more comments were submitted to the TSA though its blog, but not published.

Since the only notice of the new ID "requirements" provided by the TSA was on its website and in its blog, and since the only opportunity provided for public comment was on that blog, the complete record of comments on this topic submitted to the TSA blog – including those

---

9 "TSA Announces Enhancements to Airport ID Requirements to Increase Safety", June 5, 2008, <http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm>, archived at <http://web.archive.org/web/20080610051740/http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm>

10 "New ID Requirements Begin Tomorrow", June 20, 2008, <http://www.tsa.gov/blog/2008/06/new-id-requirements-begin-tomorrow.html>; "New ID Requirements: The First 48", June 23, 2008, <http://www.tsa.gov/blog/2008/06/new-id-requirements-first-48.html>; "ID Update and Word on the Blog", June 27, 2008, <http://www.tsa.gov/blog/2008/06/id-update-and-word-on-blog.html>; all archived at <http://web.archive.org/web/20080630050739/http://www.tsa.gov/blog>.

that weren't published – is part of the administrative record of this rulemaking which should be made public and submitted to OMB for consideration.

Notwithstanding the absence of statutory authority, rulemaking, or rules, the TSA and its contractors began asking selected air travelers to complete the form later known as TSA Form 415, and collecting additional information verbally from them, on June 21, 2008.[11]

On information and belief – based on published incident reports[12], unpublished reports provided to the Identity Project, and TSA reports disclosed to the Identity Project (and discussed further below), in most or all cases when a traveler is asked or required to complete Form 415 or its unnumbered predecessor form(s), the traveler is also asked a selection of questions from a standard list, the answers to which are compared with records from a commercial data broker.[13]

The day the TSA began using this form, June 21, 2008, the Identity Project requested "a copy of TSA's new identification requirement and all documents relating to it," pursuant to the Freedom Of Information Act (FOIA), and requested expedited processing of that request.[14]

---

11 See, "First Reports Of What It's Like Flying Without ID Arrive", June 24, 2008, <https://papersplease.org/wp/2008/06/24/first-reports-of-what-it%e2%80%99s-like-flying-without-id-arrive/>. What we believe to be the first version of the form later known as TSA Form 415 was first published by the Identity Project on our website on July 28, 2008, at <https://papersplease.org/wp/2008/07/28/dhs-ignores-omb-government-approval-process-on-tsa%e2%80%99s-questionnaire-form-for-travelers-without-id/> and as part of a blog post the same day, "DHS Ignores OMB Government Approval Process on TSA's Questionnaire Form for Travelers Without ID", July 28, 2008, <https://papersplease.org/wp/2008/07/28/dhs-ignores-omb-government-approval-process-on-tsa%e2%80%99s-questionnaire-form-for-travelers-without-id/>. So far as we know, no version of Form 415 or of any of its unnumbered predecessor(s) has ever been published by the TSA.

12 See e.g. "First Reports Of What It's Like Flying Without ID Arrive", June 24, 2008, <https://papersplease.org/wp/2008/06/24/first-reports-of-what-it's-like-flying-without-id-arrive/>.

13 See, "Accurint exposed as data broker behind TSA 'ID verification'", November 9, 2015, <https://papersplease.org/wp/2015/11/09/accurint-exposed-as-data-broker-behind-tsa-id-verification/>. An identity thief familiar with the data broker's records pertaining to an individual would typically be better able to tell the TSA or TSA contractors what the data broker's file alleges than would the actual individual, who probably has never seen the data broker's records and has no idea what inaccurate allegations they contain.

14 FOIA request later assigned request number TSA08-0723, <https://papersplease.org/wp/wp-content/uploads/2008/06/tsafoiareq62108_final.pdf>, discussed in and linked from blog post, "TSA Changes Airport ID Requirement; ID-Less Could Be Denied Right to Fly", June 23, 2008, <https://papersplease.org/wp/2008/06/23/tsa-changes-airport-id-requirement-id-less-could-be-denied-right-to-fly/>.

Despite the FOIA deadline and the request for expedited processing, the TSA did not produce any responsive documents until more than six months later. On January 12, 2009, the TSA provided us with five redacted pages of excerpts from the TSA "Screening Management SOP", Revision 3, May 28, 2008 (Implementation Date: June 30, 2008), "Appendix 2: Travel Document and ID Checks".[15] Notably, the TSA's response to this FOIA request did not include any version, even in redacted form, of the form later known as TSA Form 415, even though the form was clearly responsive to our request for all "documents relating to" the ID requirement and could not plausibly be claimed to be exempt, in its entirety, from disclosure pursuant to FOIA. There was no mention in these records of any request for OMB approval for this form.[16]

On January 31, 2011, we made another request, pursuant to FOIA, for "the most recent version of the document" later known as TSA Form 415 and "any records related to requests for approvals of this form by OMB, any OMB control number assigned to any version of this form, or the potential need for such approval."[17]

This time, the TSA delayed responding for even longer, more than two years. Finally, on May 9, 2013, the TSA disclosed a version of one side of "TSA Form 415, August 2008 [File: 400.7.2]", with no OMB control number or PRA notice, and 51 redacted pages of email messages, some of them discussing Form 415 as a two-sided form although no portion of any version of the back side of the form was disclosed.[18]

---

15 Later published at <http://www.papersplease.org/wp/wp-content/uploads/2009/05/tsa_id_sop.pdf>, linked from and discussed in blog post, "TSA releases (censored) ID checking procedures", May 26, 2009, <https://papersplease.org/wp/2009/05/26/tsa-releases-censored-id-checking-procedures/>.

16 See discussion of this and other requirements in our blog, "TSA 'identity verification' procedures", July 8, 2008, <https://papersplease.org/wp/2008/07/08/tsa-identity-verification-procedures/>.

17 Later designated as FOIA request TSA11-0344.

18 Form 415 at <http://papersplease.org/wp/wp-content/uploads/2013/05/tsa-form-415.pdf>; FOIA response at <https://papersplease.org/wp/wp-content/uploads/2013/05/tsa11-0344-response-9may2013.pdf>, linked from and discussed in blog post, "TSA never got OMB approval for 'Certification of ID' (Form 415)", May 29, 2013, <https://papersplease.org/wp/2013/05/29/tsa-never-got-omb-approval-for-certificate-of-id-form-415/>.

One of the email messages included in that response to our FOIA request was from "OIMP Director" (sender and recipient email addresses redacted), dated February 10, 2011, and was apparently sent in response to our FOIA request. The "Subject:" header, unredacted, was "Re: 3600 - FOIA, Request TSA11-0344 (REPLY/NOTICE)".

This message[19] stated:

> Relative to **TSA Form 415, Certification of Identity**, indications were the form was to be completed by TSA officials via phone collection rather than issued to persons to complete. Consequently, it was understood that Paperwork Reduction Act (PRA) was not applicable and OSO, as the requesting office, did not request PRA (OMB submission).
>
> For questions re: PRA, pls contact OIT's [redacted], TSA PRA Officer.

It's obvious by inspection of the form that no competent person who had seen the form could have made this statement in good faith. Every version of the form has had a line for the signature of the individual traveler, and it is not credible that anyone believed that "TSA officials via phone collection" were expected to sign the form in the name of the traveler.

To summarize this history, the current notice of TSA intent to seek OMB approval for continued use of TSA Form 415 comes after many years of TSA withholding of the form itself and the policies (if any) related to its use, even when they were specifically requested; failure to provide public notice or opportunity for public comment on these "requirements"; and failure to submit any version of this form for OMB approval, even when that was considered and when multiple versions of the (unapproved) form had been in use for many years.

---

19 Available at <https://papersplease.org/wp/wp-content/uploads/2013/05/tsa-form-415-omb.pdf>, linked from and discussed in blog post cited in Note 11, *supra*.

VI. THE CURRENT USE OF FORM 415 AND THE ADDITIONAL ASSOCIATED INFORMATION COLLECTION VIOLATE THE PAPERWORK REDUCTION ACT.

The Paperwork Reduction Act, 44 USC § 3507 (a)(1), provides that, "An agency shall not conduct or sponsor the collection of information unless in advance of the adoption or revision of the collection of information, (1) the agency has" carried out a series of steps, none of which have yet been taken with respect to TSA Form 415, "(2) the Director [of OMB] has approved the proposed collection of information … ; and (3) the agency has obtained from the Director a control number to be displayed upon the collection of information."

The PRA further provides that, "Notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information that is subject to this chapter if – (1) the collection of information does not display a valid control number assigned by the Director [of OMB] in accordance with this chapter; or (2) the agency fails to inform the person who is to respond to the collection of information that such person is not required to respond to the collection of information unless it displays a valid control number." (44 USC § 3512)

The TSA is an agency subject to the PRA. Freedom of travel is a right, and denial or interference with air travel by common carrier is clearly a "penalty" within the meaning of this section of the PRA.

Each time since 2008 that TSA employees or contractors, or local law enforcement officers relying on (false) allegations by TSA staff or contractors that completion of Form 415 or responses to additional standardized verbal "ID verification questions" were "required" by Federal law or TSA regulation as a condition of passage, have delayed, detained, or prevented a

would-be traveler from passing through a TSA or contractor checkpoint or boarding a common carrier airline flight, they have acted in flagrant violation of the PRA (in addition to other Federal statutes and Constitutional and human rights treaty provisions).

How often has this happened, during the years that TSA Form 415 and the associated verbal information collection from travelers have been in use? We don't know, although we have made diligent efforts to find out, and are entitled to know.

No portion of the administrative record that should have been considered by the agency decision-maker (and which it would be arbitrary and capricious not to have considered), made available to the public for comment, and reviewed by OMB and any eventual reviewing court, has been published by the TSA. As with TSA Form 415 itself, and the list of questions used for the associated verbal information collection, records of the actual experience of use of TSA Form 415 and the associated verbal information collection have been made available to the public *only* to the extent that they have been obtained and posted online by the Identity Project.

Meaningfully informed agency decision-making, public comment, or review of forms and practices that have been engaged in since 2008 cannot be conducted without access to the agency's records of those many years of agency experience and its impact on the public. These records must be made available to the public by the TSA, and an opportunity provided for the public to comment on them and use them as the basis for informed comment on any proposed rules or information collection, before OMB can properly review or approve this request.

The TSA's May 9, 2013 response to our FOIA request TSA-11-0344,[20] included an example of a "TSOC ID Verification Report". On June 14, 2013, we requested all records pertaining to any such report "or similar log, record, report, or e-mail message indicating the

20 See Note 10, *supra*.

numbers of ID checks, numbers of ID checks resulting in a 'not verified' outcome, or numbers of checks resulting in a 'denied' outcome, including but not limited to any aggregated reports for these quantities over any time periods, any guidelines or instructions for the preparation of such reports or the categorization of events or outcomes for reporting purposes, and any e-mail messages mentioning such reports or reporting protocols."[21]

The TSA again dragged its feet, this time for almost two years, before beginning to respond. We received a first (redacted and badly munged) interim response on May 6, 2014. Three and a half years after we made our request, the TSA still has not completed its response.[22]

This request stated, "With respect to any e-mail messages included in the responsive records, I specifically request access to and copies of the complete informational content of the underlying electronic records, in their full and complete form including all headers and attachments, fully expanded e-mail addresses, full addresses for address 'aliases', full lists for 'distribution list' aliases, and all related metadata." In extensive discussions with the TSA FOIA office during the years this request has been pending, we have repeatedly requested that access to

---

21 FOIA request later designated 2013-TSFO-01016, June 14, 2013, <https://papersplease.org/wp/wp-content/uploads/2013/06/ foia-tsoc-id-verify-report.pdf>, linked from and discussed in blog post, "How many people fly without ID? How many are denied the right to fly?", June 14, 2013, <https://papersplease.org/wp/ 2013/06/14/how-many-people-fly-without-id-how-many-are-denied-the-right-to-fly/>. Copies of this FOIA request and all interim responses to date are at <https://archive.org/details/TSOC-ID-Verification-Reports>.

22 The TSA's "Check Status of [FOIA] Request" Web page, <https://www.dhs.gov/foia-status> has generally shown a date one month in the future, which is moved back each month by another month. It appears to be a robotic sham, not based on actual estimates. It's often completely broken. As of this writing, for example, it displays the following "status" information and expected date of completion of agency action for this request:

> "The number you entered is 2013-TSFO-01016
> Request Number: 2013-TSFO-01016
> Received Date: 06/20/2013
> Request Status: Documents Added
> Estimated Delivery Date: 12/27/2016
> Closed Date:
> Check performed on 01/05/2017 12:12:22 AM EST
> Status information is current as of 01/04/2017"

In other words, the "current" TSA estimate is that its response will be completed in *negative* one week's time. Estimates of the TSA's belief in its ability to travel backward in time are not useful to FOIA requesters.

and copies of all responsive electronic records be provided in their native form, as bitwise copies of the records as found on digital devices or storage media.

The TSA has yet to provide any responsive email messages, in any format.

Instead of complying with the requirement of the FOIA statute to produce responsive records in any format in which they are requested and can readily be reproduced (it is obviously easier to to reproduce electronic files as bitwise digital copies than in any other format), the TSA appears to have followed the following munging and substitution procedure: (1) Extract each attached file and separate it from the email message, (2) view the extracted file in an application (such as a word processing program, spreadsheet application, etc.) in "print view" mode, (3) capture a screenshot image of each "page" of the "print view" of the file, (4) create a new PDF file, (5) paste the screenshot images into the new PDF file, in random (or unexplained) order, and then (6) substitute the newly-created PDF image file for the underlying electronic records.

This procedure strips out all file metadata, and replaces text and tabular data with images. It obfuscates the structure and format of the underlying records, and greatly complicates the task of parsing, tabulation, or statistical analysis of the records. And it wastes agency time and effort, delaying the already overdue agency response to the FOIA request.[23]

---

23 The TSA's record of bad faith, delay, failure to produce records in the requested format, and substitution of newly-created (and less useful) records for responsive records should be assessed in the context of the TSA's record of personal animus and actual malice, explicitly stated in writing in the TSA's own records (obtained and published by the Identity Project) toward individuals associated with the Identity Project and these requests. See "How the TSA treats FOIA requesters it doesn't like", September 5, 2013, and documents linked from that article including libelous email message to staff of the TSA FOIA office from TSA Privacy Officer Peter Pietra, December 17, 2009, <https://papersplease.org/wp/wp-content/uploads/2013/09/pietra-17dec2009.png> and our appeal of the TSA's "response" to FOIA request TSA10-0676, <https://ia601003.us.archive.org/0/items/TSA100676AppealAttach4SEP2013/TSA10-0676-appeal-attach-4SEP2013.pdf>.

Whatever the causes for the TSA's delay and failure to date to properly process and respond to this FOIA request, the comment period should be extended until at least 60 days after the completion of this response, including any administrative appeal and/or judicial review.

While the administrative record available to us for review and comment is incomplete, the redacted and munged fragments disclosed to date by the TSA provide significant clues as to the nature, scope, and inappropriateness of the ongoing verbal information collection ("administrative interrogation") of travelers by the TSA.

Although the TSA has never sought – and even now is not explicitly seeking – OMB approval for this verbal information collection, OMB approval was and still is required.

The PRA explicitly applies to all information collection, "regardless of form or format":

> [T]he term “collection of information” … means the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for … answers to identical questions posed to, or identical reporting or recordkeeping requirements imposed on, ten or more persons, other than agencies, instrumentalities, or employees of the United States.[24]

It appears from the TSA records disclosed to date that identical questions have been posed to ten or more individuals by TSA staff and contractors, including without limitation:[25]

1. Names of Other Residents at Address?
2. Neighbor’s Names?
3. Names of Associates
4. Phone Number?
5. Judicial District?

---

24 44 U.S. Code § 3502(3)(A).

25 See, "How does the TSA decide if you are who you say you are?", June 9, 2016, <https://papersplease.org/wp/2016/06/09/how-does-the-tsa-decide-if-you-are-who-you-say-you-are/>.

6. County of Residence?
7. Previous County of Residence?
8. Previous Address?
9. Other States of Residence?
10. Company Worked?
11. Name of Past Employer?
12. Employment History?
13. Sporting License?
14. Recreational License?
15. Mother’s Middle Name and DOB?
16. Mother’s Occupation?
17. Father’s Name and DOB?
18. Names of Relatives?
19. Relative’s Dates of Birth?
20. City of Relative’s Residence?
21. Vehicles Registered?
22. Mother’s Vehicles?
23. Relative’s Motor Vehicle Information?
24. Make and Model of Vehicle?

Being unable or unwilling to answer each of the questions above, or providing answers that the TSA considered inconsistent with the (unverified, "garbage in, garbage out") data

provided by the commercial data broker Accurint, is cited in TSA ID Verification Call Center reports as having been the basis for denial of passage through TSA or contractor checkpoints.

It would be premature and impermissible for OMB to approve this ongoing unlawful verbal information collection unless and until it is properly submitted for approval. That request should include a complete list of the standard questions proposed to be asked. But on its face, the list above strongly suggests an entirely inappropriate and overbroad program of interrogation, with no relationship to or likely utility – much less necessity – for any lawful TSA function.

VII. THE TSA GREATLY UNDERESTIMATES, WITHOUT ADEQUATE FOUNDATION, THE BURDEN OF THE PROPOSED INFORMATION COLLECTION.

According to the notice:

> TSA estimates that approximately 191,214 passengers will complete the TSA Form 415 annually. TSA estimates each form will take approximately three minutes to complete. This collection would result in an annual reporting burden of 9,561 hours.

The notice gives no indication whatsoever of the basis for these estimates, the manner in which they were calculated or derived, or the evidence (if any) supporting them.[26]

As noted above, the claim that this is a "new" information collection strongly suggests that the agency personnel preparing the notice were unaware that this information collection has been going on for more than eight years, or of the records of this extensive experience. Especially in the absence of any other disclosed basis for these estimates, they should be given little deference if they were prepared by personnel unfamiliar with the extensive existing records.

26 We find it especially odd that an estimate presented entirely without supporting evidence or a description of the estimating methodology is specified to a precision of six significant digits.

As discussed above, many of those those records – which include more than eight years of reports to TSA headquarters records of the duration, to the minute, of each incident in which a traveler is required to complete TSA Form 415 – have been unlawfully withheld from us despite having been requested more than three years ago pursuant to FOIA.

However, the records that have been disclosed by the TSA to date in partial response to our FOIA request[27] suggest that the TSA's estimate of three minutes per incident is far too low. As discussed above, part of the process of "completing" Form 415 is responding to a series of questions posed by telephone by personnel at the TSA ID Verification Call Center.[28] The TSA has provided no estimate of the average time to complete this verbal information collection. Based on review of the TSOC ID Verification Reports released by the TSA to date, we believe that the average time per incident required to complete the entire information collection, including the verbal information collection and the written TSA Form 415, is closer to thirty minutes than three minutes.

It is also clear from the TSOC ID Verification Reports released by the TSA to date that the TSA's estimate of 191,214 is so much higher than the number of individuals currently being required to complete this form that it cannot have been based on these records or past experience.

Currently, the TSA requires any traveler who does not present ID credentials the TSA deems "acceptable" to complete TSA Form 415 and respond to verbal information collection.

How many travelers is that likely to be? The current number is much less than 191,214 per year. The only clue as to why that might change is the following statement in the notice:

---

27 This request and all interim responses to date are at <https://archive.org/details/TSOC-ID-Verification-Reports>.

28 Sometimes checkpoint staff hand the phone to the traveler and have the traveler speak directly with IVCC personnel. Sometimes checkpoint staff play a game of "telephone" and relay questions and answers back and forth between the IVCC and the traveler, creating a risk that errors in restatement will lead to denial of travel.

> TSA will begin implementing the REAL ID Act at airport security screening checkpoints on January 22, 2018. Starting on that day, TSA will not accept state-issued driver's licenses and other state-issued identification cards from states that are not compliant with REAL ID Act requirements unless DHS has granted the state a temporary extension to achieve compliance.

If the TSA does not accept driver's licenses or ID cards issued by states that are not compliant with REAL-ID Act requirements, all air travelers presenting driver's licenses or ID cards issued by those states will be required to complete Form 415 and answer IVCC questions.

We can only guess that the TSA's estimate is somehow derived from its political prediction of which states will eventually comply with the REAL-ID Act.

But current and historical numbers suggest that the TSA's estimate of likely state noncompliance with the REAL-ID is far too low. That estimate probably reflects wishful agency thinking about a hoped-for, but unlikely, reversal of the public sentiment reflected in state policy.

More than a decade after the enactment of the REAL-ID Act, at most twelve of 55 U.S. jurisdictions (states, U.S. territories, and the District of Columbia) might be compliant.

One of the statutory elements of the REAL-ID Act is that each state that issues any compliant driver's licenses or ID cards must, "Provide electronic access to all other States to information contained in the motor vehicle database of the State" including, "at a minimum — (A) all data fields printed on drivers' licenses and identification cards issued by the State; and (B) motor vehicle drivers' histories, including motor vehicle violations, suspensions, and points on licenses."[29]

The only system currently available, under development, or reasonably foreseeable as enabling compliance with this provision of the REAL-ID Act is the "State-to-State" (S2S) system operated by the American Association of Motor Vehicle Administrators (AAMVA). S2S

29 Real ID Act, Title II, Section 202(d)(12), available at <https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf>.

includes the national "State Pointer Exchange System" (SPEXS). SPEXS is the centralized, privatized, outsourced national ID database which includes information about each and every driver's license or ID issued by any compliant state.[30]

According to AAMVA, the first state to participate in S2S was Wisconsin in 2015.[31] Only a total of twelve states currently participate in S2S.[32] Since no state not participating in S2S has any other way to comply with the database access requirement of the REAL-ID Act, at most those twelve states – not including any of the most populous states – are currently compliant.

Many of the remaining states are barred by state constitutional provisions and/or state statutes from uploading their state ID databases to SPEXS or otherwise complying with the REAL-ID Act. Public sentiment remains opposed to a national ID card or national ID database.

In light of the low compliance more than a decade after the enactment of the REAL-ID Act of 2005, we expect that the majority of jurisdictions are likely to remain nonparticipants in SPEXS, and thus noncompliant with the REAL-ID Act, a year from now on the TSA's self-imposed "deadline" of January 22, 2018. Because those are likely to continue to include most of the most populous states, we expect that at least 75% of U.S. air travelers as of that date will continue to be residents of noncompliant states. And even if we assume that one-third of them will present a passport or some other Federally-issued ID, that would still mean that roughly half of all air travelers would be residents of noncompliant states with no "acceptable" ID. All of these travelers would be required to complete Form 415 and answer IVCC questions.

---

30 See, "How the REAL-ID Act is creating a national ID database", February 11, 2016, <https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/>.

31 Email to the Identity Project quoted in "The real state of compliance with the REAL-ID Act", February 24, 2016, <https://papersplease.org/wp/2016/02/24/the-real-state-of-compliance-with-the-real-id-act/

32 AAMVA, "State to State (S2S) Verification Services: Jurisdictions' S2S Testing & Implementation Current Status", <http://www.aamva.org/State-to-State/#Participation>, accessed January 6, 2017.

In 2015, the most recent year for which data has been released, the TSA "screened" 708 million travelers.[33] If half of them have no acceptable ID and consequently are subjected to this information collection, that would be about 350 million people a year. And if answering the IVCC questions and filling out Form 415 takes about thirty minutes per person, the total annual burden of the proposed information collection would be about 175 million hours.

That's obviously unrealistic. The real burden of this proposal is that it would create such long delays at TSA checkpoints as to effectively shut down the U.S. air transportation system. It should be assessed by OMB, and by the public, on that basis.

The TSA will undoubtedly say that this won't happen because residents of noncompliant states who don't present Federally-issued ID will simply be turned away from airports. But as discussed in Part III of these comments above, there is no statutory or regulatory basis for such TSA denial of access to travel by air.

VIII. THE CURRENT AND PROPOSED VERBAL AND WRITTEN INFORMATION COLLECTION FROM TRAVELERS VIOLATES THE PRIVACY ACT.

The Privacy Act , 5 U.S. Code § 552a (e)(7), provides that each agency shall, "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity."

33 Press release, "TSA releases 2015 statistics", January 21, 2016, <https://www.tsa.gov/news/releases/2016/01/21/tsa-releases-2015-statistics>.

As discussed above, records of how, when, and where we travel are, *per se*, records of how we exercise the right to assemble (however, whenever, and wherever we choose) guaranteed by the First Amendment. In addition, many of the questions listed above (which we only know about because records were maintained by the TSA of who was asked these questions, whether they answered, and whether their answers were deemed "acceptable") pertain to how individuals exercise rights of assembly, association, and other rights protected by the First Amendment. Questions asked of would-be travelers such as "Names of Associates?" clearly implicate the right to freedom of association, as do others of they questions mentioned in these records.

Questioning by TSA staff and contractors is an administrative interrogation, not a law enforcement function.[34] Neither most TSA checkpoint staff nor TSA contractors are law enforcement officers. So this record-keeping cannot be justified under the second fork of the Privacy Act test as, "within the scope of an authorized law enforcement activity," even if these questions were pertinent to such a purpose, which on their face they do not appear to be.

The maintenance of these records would thus be permissible under the Privacy Act only if it was "expressly authorized by statute". But whatever strained theory of *implicit* authorization the TSA may try to construct, this record-keeping is not *explicitly* authorized by any statute.

---

34 It's not clear what, if any, authority might exist for "administrative interrogation". Case law on administrative searches invariably assumes that those individuals subjected to administrative searches have the absolute right to stand mute. In the only cases of which we are aware that have upheld administrative interrogation at drunk-driving or immigration checkpoints, these have been upheld only on the basis that individuals were not required to respond to any such questions, and must be allowed to proceed after only a brief belay in the absence of evidence – independent of their silence – sufficient to support a law enforcement detention or arrest. We are aware of no case law upholding compelled responses to administrative interrogation by the TSA or its contractors, or the denial of passage by common carrier or imposition of other penalties for non-response. Statutory authority for “screening” is neither a general warrant for search nor a general subpoena for testimony. The obligation of travelers to submit to “screening” cannot validly be construed as an obligation to submit to any search or respond to any interrogatories declared by the TSA or checkpoint staff to constitute “screening”. This proceeding is not a rulemaking, but these issues would need to be addressed in the rulemaking if the TSA were to propose rules that would require travelers to respond to administrative interrogatories.

There is nothing in Federal statutes authorizing the TSA to identify travelers, much less explicitly authorizing the keeping of records pertaining to travelers' identities.

Indeed, it has been the consistent and explicit (and correct) position of the TSA itself, whenever the issue has arisen in litigation, that no Federal statute or TSA regulation requires travelers to have or display and ID credentials in order to pass through TSA checkpoints.

This was the argument made by the TSA in *Gilmore v. Gonzales*.[35] It was the TSA's own argument, and the evidence submitted by the TSA itself, *ex parte* and under seal, which persuaded the 9th Circuit Court of Appeals that Mr. Gilmore could have flown with no ID as a "selectee"[36] if he submitted to more intrusive search. That factual finding that TSA policy and practice would have allowed Mr. Gilmore to fly without ID was critical to the Court's decision that Mr. Gilmore's Constitutional right to travel had not been violated.

This was also the testimony under oath of a TSA "Lead Checkpoint Security Officer" familiar with the TSA's ID procedures in the criminal trial of *State of New Mexico v. Phillip Mocek*.[37] "You don't have to show ID. You can fly without ID. We have a procedure for that."

To the extent that the TSA's notice in the *Federal Register* explains or attempts to offer any purported justification for the proposed new ID requirement, it is the following:

> To ensure that the identity verification process described above does not become a means for travelers to circumvent implementation of the REAL ID Act, TSA is updating the process...

This is, at most, an argument that the REAL-ID Act somehow *implicitly* authorizes the TSA to impose an ID requirement to fly. It does not point to any *explicit* statutory authorization

---

35 See Notes 5-7, *supra*, and accompanying text.

36 435 F. 3d 1125 at 1133 (2007).

37 Criminal Case 2573709, Bernalillo County Metropolitan Court. No transcript of the trial was prepared. Audio recordings made by the Identity Project with the permission of the court are available at <https://papersplease.org/wp/2011/01/24/audio-state-of-new-mexico-v-phillip-mocek/>.

for such an ID requirement to fly, and thus fails to satisfy the requirements of the Privacy Act.

This statement in the notice also fundamentally misconstrues the REAL ID Act.[38]

The REAL-ID Act pertains solely to *which* ID credentials are considered acceptable for Federal purposes. The REAL-ID Act does not itself impose or change any requirements for when, where, or for what purposes ID is required. The REAL-ID Act contains no authorization for the TSA or any other agency to impose new ID requirements.

The REAL-ID Act is implicated only in circumstances in which *other* valid Federal statutes or regulations require acceptable ID. Neither when the REAL-ID Act of 2005 was enacted, nor today, does any statute or regulation purport to impose or purport to authorize the TSA to impose any such requirement for air travel.

Circumvention of the REAL-ID Act would consist of passing off some non-compliant ID as acceptable, or engaging in some activity that requires ID – like operating a motor vehicle, and unlike traveling as a passenger on a common carrier – without having ID. A traveler who has no ID, or who does not present any ID, is not representing some other ID as being compliant with the REAL-ID Act, or as acceptable for any Federal purpose. Such a traveler is doing nothing to circumvent the REAL-ID Act.

In the absence of any valid statute or regulation requiring ID to fly, the REAL-ID Act is simply not implicated by air travel by those who do not have, or do not chose to present, any ID.

Flying without ID is a lawful everyday activity. Flying without ID does not constitute circumvention of the REAL-ID Act any more than living, working, playing, moving from place to place, or engaging in any other activities of life without having been issued or being in

38 Public Law 109-13, Division B – REAL ID Act of 2005, 119 Stat. 231, 302–23 (May 11, 2005).

possession of ID credentials – where those activities are not subject to valid ID requirements as a condition of licensing or otherwise – constitutes circumvention of the REAL-ID Act.

IX. CONCLUSION AND RECOMMENDATIONS

The TSA should withdraw this application. If it does not do so, OMB should reject it. And the TSA should cease and desist from any attempt to require ID to travel by common carrier, or to claim that the REAL-ID Act of 2005 or any other Federal statute requires, or authorizes the TSA to require, that air travelers have or provide ID.

Respectfully submitted,

The Identity Project (IDP)

<http://www.PapersPlease.org>

A project of the First Amendment Project

1736 Franklin St., 9th Floor

Oakland, CA 94612

The Cyber Privacy Project

<http://www.cyberprivacyproject.org>

_____/s/_____

Edward Hasbrouck,

Consultant to IDP on travel-related issues

January 9, 2017

From: Ian Sharping
Sent: Mon, 9 Jan 2017 15:02:58 -0600
To: TSAPRA
Subject: Comment - Docket No. TSA-2013-001-0075, FR Doc. 2016-26958
Attachments: 2017.01.08_CPP_Real ID Comment_v3.0.pdf

To whom it may concern:

The Cyber Privacy Project (CPP) submits these comments in response to the notice and request for comments, "Intent To Request Approval From OMB of One New [sic] Public Collection of Information: Certification of Identity Form (TSA Form 415)", docket number TSA-2013-0001-0075, FR Doc. 2016-26958, published at 81 Federal Register 78624-78625 (November 8, 2016).

Sincerely,

Ian Sharping